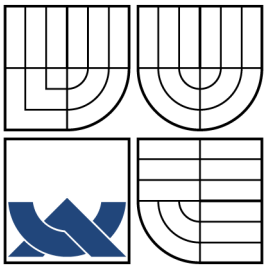
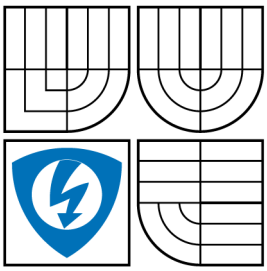


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY
A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKÁCIÍ

FACULTY OF ELECTRICAL ENGINEERING AND
COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

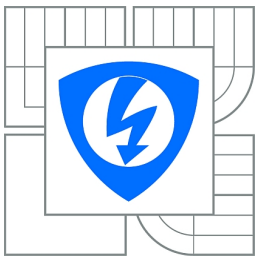
MULTICAST V IP SIEŤACH
MULTICAST IN IP NETWORKS

BAKALÁRSKA PRÁCA
BACHELOR'S THESIS

AUTOR PRÁCE — PETER PETROVSKÝ
AUTHOR

VEDÚCI PRÁCE — Ing. RADKO KRKOŠ
SUPERVISOR

BRNO 2013



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Peter Petrovský	***ID:***	136574
Ročník:	3	***Akademický rok:***	2012/2013

NÁZEV TÉMATU:

Multicast v IP sieťach

POKYNY PRO VYPRACOVÁNÍ:

Naštudujte problematiku multicast prenosov v IP sieťach, analyzujte rôzne služby bežne šírené pomocou multicast vysielania a podrobne popíšte ich požiadavky na sieťové prostriedky. Oboznámte sa s možnosťami prenosu objemného dátového obsahu ako služby prebiehajúcej na pozadí, analyzujte a popíšte existujúce takéto systémy. Preštudujte existujúce programové systémy podporujúce vytvorenie systému pre súčasnú distribúciu digitálneho obsahu na viaceré pracovné stanice v sieti s využitím multicast prenosu, navrhnite a zrealizujte takýto systém. Realizujte prenos dátového obsahu pomocou Vami navrhnutého systému, vykonajte merania a porovnajte zlepšenie voči unicast prenosu.

DOPORUČENÁ LITERATURA:

[1] WITTMANN, Ralph a Martina ZITTERBART. Multicast Communication: Protocols and Applications. San Francisco: Morgan Kaufmann Publishers, 2001, 349 s. ISBN 15-586-0645-9.
[2] PERKINS, Colin. RTP: Audio and Video for the Internet. Boston: Addison-Wesley, 2003, 414 s. ISBN 06-723-2249-8.

Termín zadání:	11.2.2013	***Termín odevzdání:***	5.6.2013

Vedoucí práce: Ing. Radko Krkoš
Konzultanti bakalářské práce:

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

ABSTRAKT

Táto bakalárska práca sa zaoberá komunikáciou typu multicast. Vysvetľuje sa v nej princíp prenosu dát pomocou multicastu. Taktiež sa zaoberá protokolom pre prihlasovanie do skupín a službami šírenými využitím multicastu. Použitím protokolu TFTP sa zrealizuje systém pre distribúciu obsahu komunikáciou typu multicast. Premerá a porovná sa rozdiel medzi unicastom a multicastom.

KĽÚČOVÉ SLOVÁ

multicast, TFTP, IGMP, Linux, cron

ABSTRACT

This bachelor's thesis deals with multicast communication. It explains the principle of multicast data transfer. It also deals with protocol for logging into groups and distributed multicast services. Using TFTP is implemented system for content distribution by multicast communication. It measure and compare the difference between unicast and multicast.

KEYWORDS

multicast, TFTP, IGMP, Linux, cron

PETROVSKÝ, Peter *Multicast v IP sieťach*: bakalárska práca. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikácií, 2013. 54 s. Vedúci práce bol Ing. Radko Krkoš

PREHLÁSENIE

Prehlasujem, že som svoju bakalársku prácu na tému „Multicast v IP sieťach“ vypracoval samostatne pod vedením vedúceho bakalárskej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej bakalárskej práce ďalej prehlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúceho autorského zákona č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka č. 40/2009 Sb.

Brno ....

(podpis autora)

POĎAKOVANIE

Rád by som poďakoval vedúcemu bakalárskej práce pánovi Ing. Radkovi Krkošovi za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci.

Brno ....

(podpis autora)

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ÚVOD

Unicast v dnešnej dobe plnej pokroku nie je dostačujúcou technológiou pri prenose dát a hlavne digitálneho obsahu. Jeho nevýhoda sa najvac ukazuje pri použití v prípade prenosu tých istých dát z jedného bodu k mnohým. Zaťažuje totiž šírku pásma nadbytočným prenosom, keďže každý prenos je realizovaný osobitne od bodu k bodu. V mojej bakalárskej práci sa preto budem zaoberať technológiou multicast, ktorý rieši tento problém. Popíšem spôsob komunikácie v sieťach, adresovania multicastu v sieti a spôsob prihlasovania do skupín. Budem sa zaoberať službami bežne šírenými pomocou multicast, kde sa zameriam hlavne na požiadavky kladené na sieťové prostriedky. Ďalej popíšem prenos dát pomocou technológie TFTP, ktoré bude prebiehať ako služba prebiehajúca na pozadí. Realizujem prenos dát pomocou unicast a multicast prenosu. Vzájomne ich porovnám a zameriam sa hlavne na výhody multicast prenosu oproti unicast prenosu. Nakoniec navrhnem systém pre súčasnú distribúciu obsahu na viaceré pracovné stanice pomocou multicastu, ktorý bude fungovať automatizovane.

1 KOMUNIKÁCIA V SIEŤACH

Rozľahlé siete môžeme realizovať dvomi spôsobmi, buď prepojovaním okruhov, alebo prepojovaním paketov (paketovo komutované siete). V sieťach s prepojovaním okruhov sa komunikácia odohráva po dopredu zostavenom okruhu medzi odosielateľom a príjemcom, kde sú všetky dáta doručené v správnom poradí. Komunikácia v týchto sieťach prebieha vždy spoľahlivo, so spojením. Príkladom realizácie je telefónna sieť alebo ISDN. [20]

1.1 Paketovo komutované siete

Základom paketovo komutovaných sietí je prepojovanie paketov v jednotlivých prepojovacích uzloch na tretej, prípadne druhej vrstve (teda smerovačoch či prepínačoch), kde sa cesta hľadá a určuje nezávisle v každom takom uzle. Smerovanie je možné nastaviť dynamicky alebo staticky. V prípade dynamického smerovania každý paket v rámci danej komunikácie putuje nezávisle, teoreticky rôznou cestou – podľa stavu topológie siete, jej priechodnosti a výpadku na trase. Všetky tieto záležitosti totiž ovplyvňujú voľbu ďalšej cesty v smerovačoch, ktoré musia na každú zmenu reagovať dynamicky. Paket je odoslaný bez predbežného zistenia, či existuje cieľový uzol, bez zostavovania cesty a jeho sledovania, či k cieľu dorazil. Preto každý paket musí byť plne vybavený všetkými údajmi, potrebnými pre jeho odoslanie k cieľu: cieľovou adresou, prípadne požadovanou úrovňou kvality služby a ďalšími voliteľnými možnosťami. Každý paket sa smeruje nezávisle na ostatných a jeho kópie môžeme prenášať na niekoľko cieľových adries (multicast či broadcast). Prepojovanie paketov sa dnes používa v lokálnych sieťach (LAN, Local Area Network), ale aj v rozľahlých sieťach (WAN, Wide Area Network). Prepojovanie paketov sa vo svojej klasickej podobe využívalo v rozľahlých sieťach X.25. Z prepojovania paketov premennej dĺžky (na tretej vrstve, L3) sa postupne vyvinulo prepojovanie rámcov premennej dĺžky (na druhej vrstve, príkladom Frame Relay) a nakoniec prepojovanie buniek konštantnej dĺžky (L1/2, príkladom ATM). Komutovanie paketov môžeme realizivať bez spojenia (založené na datagramových správach) alebo virtuálnym prepojovaním okruhov (tiež známe ako so spojením).

Oproti prepojovaniu okruhov má komutovanie paketov radu výhod. Napríklad sa nevyžaduje, aby koncové zariadenia, komunikujúce mezi sebou, boli rovnakého typu (mali rovnakú prenosovú rýchlosť, rovnaký spôsob prenosu, pracovali rovnakou abecedou a kódom). Pakety v sieti postupujú po kratších prenosových úsekoch, ktoré sú spoľahlivejšie a kvalitnejšie (majú menšiu chybovosť). Pokiaľ by ani táto úroveň nevyhovovala, potom stačí použiť niektoré doplnkové mechanizmy na jednotlivých

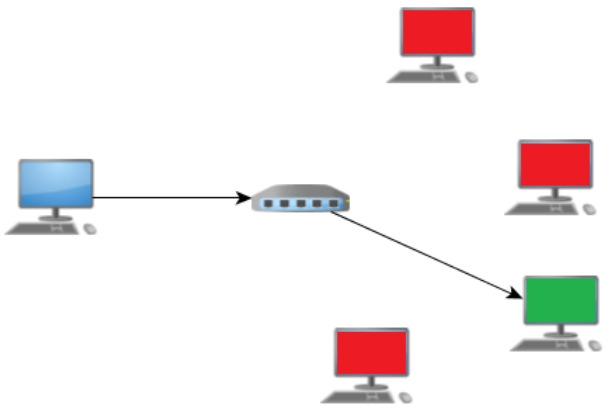
úsekoch a nie na celom okruhu medzi komunikujúcimi koncovými uzlami (na celej ceste sieťou), ako je tomu v komutačných sieťach. Paketová komunikácia umožňuje zadržanie paketov v sieti pri absencii adresáta alebo ich prevedeniu po dohode s adresátom na iný koncový uzol. Veľkou výhodou je aj cena, ktorá je výrazne nižšia ako v prípade oruhovo komutovanej siete. Nevýhodou komutovania paketov je vyššia réžia (záhlavie u každého paketu). [21]

1.2 Druhy komunikácie

V rámci komunikačnej skupiny sa môžu rôzne typy komunikácie líšiť v závislosti od počtu odosielateľov a príslušných príjemcov. V IP sieťach poznáme štyri typy komunikácie z pohľadu príjemcov: unicast, broadcast, multicast a anycast.

1.2.1 Unicast

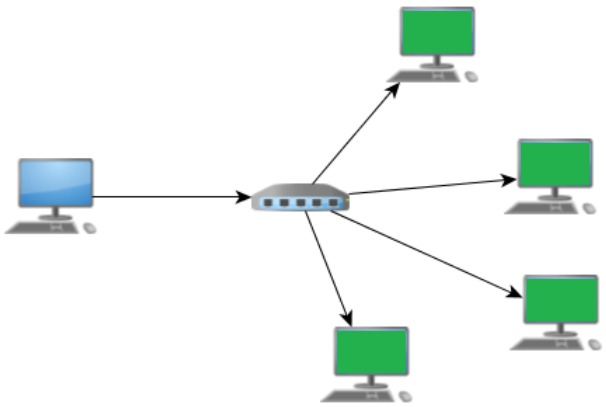
Unicast (obr. 1.1) je ekvivalentom k tradičnej bod-bod komunikácií, kde je len jeden odosielateľ a jeden príjemca. Je to najbežnejší spôsob komunikácie v internete. V súčasnej dobe však nie je vhodný pre všetky typy komunikácie. Hlavne pre tie, kde je viac zdrojov a viac príjemcov, pretože zdroj by musel zaslať dáta toľkokrát, koľko je príjemcov. To by mohlo viesť k zbytočnému plytvaniu prenosových prostriedkov siete (napr. šírka pásma) i prostriedkov zdroja samotného, ktorý by musel niekoľkokrát zaslať rovnaké dáta.



Obr. 1.1: Unicast.

1.2.2 Broadcast

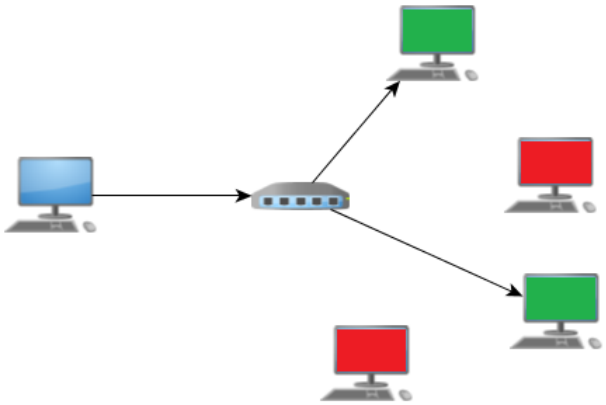
Broadcast (obr. 1.2) je ďalším typom komunikácie, ktorý je porovnateľný s multicastom, keďže existuje len jeden odosielateľ. Avšak pri broadcaste nie je žiadne obmedzenie, pokiaľ ide o skupiny prijímačov, dáta sú posielané všetkým potenciálnym príjemcom. Broadcast nevyžaduje zriaďovanie, adresovanie, či administráciu. Pokiaľ sieť nie je vhodným spôsobom rozdelená na podsiete alebo chránená (napr. firewallom), môžu broadcast správy spôsobiť zahltenie siete.



Obr. 1.2: Broadcast.

1.2.3 Multicast

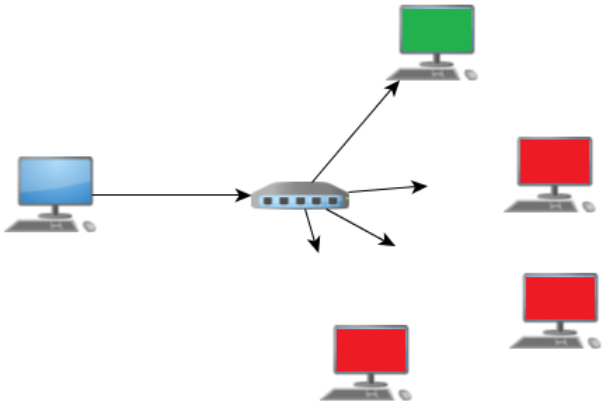
Multicast (obr. 1.3) poskytuje lepšiu možnosť komunikácie z pohľadu úspory sieťových prostriedkov pre jedneho odosielateľa a viac príjemcov alebo viac odosielateľov a viac príjemcov, pričom sa nevyžadujú predchádzajúce znalosti o tom, koľko príjemcov existuje. Efektívne využíva sieťovú infraštruktúru tým, že od odosielateľa odošle dáta iba raz, aj keď je potrebné dodať dáta veľkému počtu príjemcov. Kópie dát sa vytvárajú vždy v smerovačoch umiestnených najbližšie k danému príjemcovi, aby sa čo najviac šetrili prenosové prostriedky siete. Pokiaľ má príjemca záujem prijímať dáta, musí sa najskôr prihlásiť do danej skupiny.



Obr. 1.3: Multicast.

1.2.4 Anycast

Anycast (obr. 1.4), podobne ako broadcast a multicast, je založený na topológii typu jeden odosielateľ a viac príjemcov. Avšak v tomto prípade sú dáta od jedného odosielateľa smerované do topologicky najbližšieho uzlu v skupine potenciálnych prijímačov určených rovnakou cieľovou adresou. V súčasnosti sa anycast hojne využíva pre koreňové DNS servery, kde jediná adresa je priradená aj niekoľkým desiatkam fyzických serverov a DNS zisťovanie je doručené vždy najbližšiemu z nich.



Obr. 1.4: Anycast.

2 IP MULTICAST

IP multicasting je prenos IP datagramu na „hostiteľskú skupinu“. Je sadou viacerých hostiteľov identifikovaných jedinou cieľovou adresou. Členstvo v skupine je dynamické, to znamená, že hostia sa môžu pripojiť a odísť zo skupiny kedykoľvek. Neexistuje žiadne obmedzenie na umiestnenie alebo počet členov v skupine, pričom hostiteľ môže byť členom viac ako jednej skupiny naraz. Hostiteľská skupina môže byť stála alebo prechodná. Stála skupina má dobre známu, administratívne pridelenú IP adresu. Môže mať ľubovoľný počet členov, dokonca nula. Tie IP multicast adresy, ktoré nie sú vyhradené pre stále skupiny, sú k dispozícii pre dynamické prideľovanie prechodných skupín, ktoré existujú iba tak dlho, kým majú členov. Bližšie sa touto problematikou zaoberá špecifikácia RFC 1112. [6]

2.1 Adresovanie v multicaste

Adresy, ktoré spadajú do rozsahu od 224.0.0.0 do 239.255.255.255 (rozsah triedy D), sú známe ako multicast adresy. Všetky multicast adresy sú registrované priamo v IANA (Internet Assigned Numbers Authority). Prostredníctvom normálnych procesov IETF (Internet Engineering Task Force) pridelil niekoľko multicast adries pre špeciálne účely.

Adresný blok 224.0.0.0/24 je určený na komunikáciu iba na lokálnej podsieti. Nachádzajú sa tu napríklad protokoly riadenia prevádzky (napr. RIPv2 používa 224.0.0.9). Smerovače nesmú odovzdať tieto datagramy mimo podsiete, z ktorej pochádzajú.

Blok adries 224.0.1.0/24 (tzv. Internetwork Control Block) sa používa pre komunikáciu, ktorá musí byť smerovaná cez verejný internet. Zvyšok adresného priestoru 224.0.0.0/8 je priradený rôznym aplikáciam, ktoré sú používané niekoľko rokov alebo si ich IANA jednoducho vyhradila.

Blok 232.0.0.0/8 je vyhradený pre SSM (Source Specific Multicast). Ďalší blok adries 233.0.0.0/8 je tzv. GLOP blok. Adresy v tomto bloku sú globálnym rozsahom staticky priradených adries. Priradenie sa vykonáva mapovaním doménových ASN (Autonomous System Number) do stredu dvoch oktetov 233.X.Y.0/24. Bližšie je mapovanie a priraďovanie adries definované v RFC 2770 [15].

Rozsah 239.0.0.0/8 je priradený RFC 2365 [16] pre súkromné použitie v rámci organizácie. Pakety určené do administratívneho rozsahu multicastových adries nekrižujú administratívne definované hranice organizácie a adresy sú lokálne zadané a nemusia byť globálne jedinečné. Sú povahovo privátne.

Zvyšok adries adresného rozsahu triedy D je označený organizáciou IANA ako rezervovaný. [1]

2.1.1 Adresovanie na spojovej vrstve (L2)

Unicast pakety sú doručované na konkrétneho príjemcu ethernetovej podsieti nastavením určitej MAC adresy na IP adresu paketu. Broadcastove pakety využívajú broadcastovu MAC adresu (ff:ff:ff:ff:ff:ff), ktorá obsahuje nastavenie broadcastového/multicastového bitu v adrese. IANA vyčlenila pre IPv4 multicasting rozsah MAC 01:00:5e:00:00:00 až 01:00:5e:7f:ff:ff. Prvých 25 bitov v každej MAC adrese má fixnú hodnotu, ktorá sa musí dodržať. Zostávajúcich 23 bitov v MAC slúži na popísanie multicastovej skupiny. Bežné IP adresy sa mapujú pomocou ARP (Adress Resolution Protocol), tento princíp neplatí o adresách triedy D. Spodných (koncových) 23 bitov multicastovej IP adresy sa prenesie do spodných 23 bitov multicastovej MAC adresy. To znamená, že jednej MAC adrese zodpovedá 32 rôznych IP adries (224.1.1.1, ..., 239.129.1.1). Ak prepínač nerozumie multicast adresám, potom prevádzka bude vysielaná broadcastom na multicastovú skupinu všetkých členov siete. V tomto prípade systémová sieťová karta (alebo operačný systém) musí filtrovať pakety odoslané na porty, cez ktoré nie je vyžiadaný multicast prenos. [23]

2.2 Modely multicastu

Pôvodná verzia podpory multicastu podľa RFC 1112 [6] podporovala model one-to-many a many-to-many. Na podporu druhého prípadu je potrebné zistiť zdroj vysielania, ktorý je v prvom prípade známy. Tento model vysielania sa označuje ako ASM. V poslednej dobe, kedy sa multicast stáva stále zaujímavejší na internete aj pre komerčné aktivity, sa efektívne redukuje ASM na vysielanie z jedného zdroja. Tento menej zložitý model sa nazýva SSM. [4]

2.2.1 ASM (Any Source Multicast)

V tejto komunikácii je využívaný zdieľaný strom. Zdieľaný strom je pre celú skupinu rovnaký a môže do neho patriť jeden alebo viac zdrojov. Jeho koreň je umiestnený do jedného bodu siete nazývaného Redenzvous point (RP). Pri komunikácii sú dáta smerované od zdroja k RP a následne k prijímačom. Zdieľané stromy sú označované (*,G), kde * znamená, že strom nie je závislý na zdroji multicastu a G označuje multicastovu adresu.

Komunikácia v ASM:

- Koncové zariadenie vyšle svojmu smerovaču paket IGMP so žiadosťou o príjem vysielania zo zvolenej multicastovej adresy.

- Koncový smerovač požiada o príjem multicastového koreňa RP (buď je nastavený staticky alebo pomocou Auto-RP, kde smerovač odošle dáta na adresu 224.0.1.39 alebo 224.0.1.40).
- RP začne vysielať koncovému zariadeniu dáta od zdroja multicastového vysielania.
- Po prvom prijatom pakete môže koncové zariadenie vypočítať najkratšiu cestu ku zdroju a pakety potom môžu byť smerované touto cestou. RP slúži len na to, že sa smerovač dozvie o umiestnení zdroja vysielania. [4]

2.2.2 SSM (Source Specific Multicast)

Source Specific Multicast využíva skupinu multicastových adries v rozsahu 232.0.0.0/8. Komunikácia je založená na zdrojovom strome, tzv. strome najkratších ciest (SPT – Shortest Path Three). Zdroj vysielania je vždy koreň a smerovače na ceste sú listy (príjemcovia). Pre tieto stromy sa používa označenie (S,G), kde S (Source) je zdroj a G označuje multicastovu adresu. Z toho plynie, že pokiaľ je v jednej skupine viac zdrojov, tak pre každý zdroj existuje viac stromov. U SSM je teda možné používať jednu multicastovu adresu pre viac skupín. Je tu odstránený problém s alokáciami adries a nedostatočným riadením prístupu. [4]

Komunikácia v SSM:

- Koncové zariadenie vyžiada od koncového smerovača multicastové vysielanie z multicastovej adresy a zadá zdroj, od ktorého vysielanie prijímať.
- Je zostavený strom od vysielača až k prijímaču.

2.3 Registrácia do skupín

IGMP bolo zavedené pre skupinové riadenie v rámci podsietí alebo okrajových sietí. Definuje, ako sa pripojiť do skupiny alebo opustiť skupinu a poskytuje informácie o existujúcich skupinách. IGMP dátové jednotky sú počas prenosu zapuzdrené do IP datagramov. V tomto zmysle je IGMP logicky umiestnený nad IP protokolom. Všetky dátové jednotky sú odosielané s TTL (time to live) rovným 1, čo znamená, že neopustia lokálnu podsieť. IGMP prešlo niekoľkými verziami: verzia 1 (RFC 1112) a verzia 2 (RFC2236) [10]. Súčasná, už tretia, verzia je špecifikovaná v RFC 3376 [3]. IGMP vo všeobecnosti využíva tri druhy správ:

Membership Query, ktoré sa ďalej delí na general a group-specific. General sa používajú na získanie informácií o skupinách, ktoré majú členov v pripojenej podsieti. Operácia group-specific kontroluje, či konkrétna skupina má členov v podsieti. Tieto

správy sú pravidelne odosielané z query smerovača do skupiny všetkých koncových systémov (všetky hostiteľské skupiny).

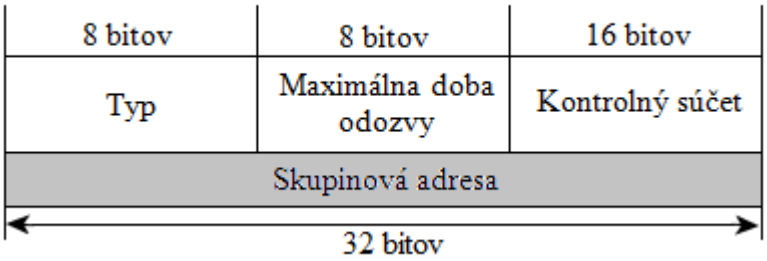
Druhým typom správ je *Membership Report*, ktorý informuje multicast smerovače o nových členstvách. Koncové systémy odpovedajú membership report na membership query vydaný multicast smerovačom. Multicast smerovač potom zaznamená túto informáciu o skupinových členstvách a nastaví skupinový časovač na skupinový interval. Táto hodnota zodpovedá času, ktorý musí uplynúť predtým, než multicast smerovač rozhodne, že skupina nemá žiadnych zostávajúcich členov v podsieti.

Posledným typom správ je *Leave Group*, ktorý signalizuje, že skupinové členstvo bolo ukončené. Je veľmi dôležitá, zlepšuje možnosti ukončenia členstva v skupine, ktoré je dôležité pre vysoko dynamické skupiny. [23]

Formát IGMP dátových jednotiek je ukázaný na obr. 2.1. Kľúčovým komponentom sú skupinová adresa a kontrolný súčet. Pole typ je použité na identifikáciu prenášaných IGMP dátových jednotiek. Typové hodnoty sú definované naslednovne:

- 0x11 pre membership query (posiela sa na adresu 224.0.0.1)
- 0x22 pre membership report verzie 3 (posiela sa na adresu skupiny)
- 0x16 pre membership report verzie 2 (posiela sa na adresu skupiny)
- 0x12 pre mebership report verzie 1 (posiela sa na adresu skupiny)
- 0x17 pre leave group (posiela sa na adresu 224.0.0.2)

General a group-specific membership query sú ďalej rozlíšené skupinovou adresou. Použitie maximálnej doby odozvy umožňuje reguláciu oneskorenia (t.j. čas medzi tým, ako posledný člen opustí skupinu a tým, kedy smerovací protokol informuje o tejto skutočnosti). [19]



Obr. 2.1: Formát IGMP dátových jednotiek.

2.3.1 IGMPv1

IGMP verzia 1 je jednoduchý protokol skladajúci sa z dvoch správ [6]:

Host Membership Report

Po pripojení hostiteľa k multicastovej skupine, hostiteľ odošle Host Membership Report na konkrétnu adresu. Na rozdiel od multicast smerovača, hostiteľ nemá prehľad o členstve ostatných hostiteľov na jeho podsieti. Vzhľadom k tomu multicast smerovač načúva v multicastovom promiskuitnom režime, prijíma a spracováva Host Membership Report správy zaslané na akúkoľvek multicast adresu.

Host Membership Query

Multicast smerovač periodicky vysiela Host Membership Query správy na 224.0.0.1 (všetci hostitelia v skupine) na obnovu svojich vedomostí o členoch v podsieti. Pre každú skupinu jeden člen skupiny odpovie Host Membership Report správou. Ako už bolo povedané, je použitý náhodný časovač odpovede k rozloženiu a náhodnému distribuovaniu člena skupiny, ktorý odošle Host Membership Report správu pre každú skupinu.

2.3.2 IGMPv2

IGMP verzia 2 rozširuje funkčnosť IGMP pri zachovaní spätnej kompatibility s IGMP verziou 1. Používa jednoduchý volebný proces pri výbere multicast query, jeden smerovač v každej podsieti, ktorý posiela pravidelné Host Membership Query správy. Smerovač s číselne najnižšou IP adresou je zvolený multicast query. Volebný proces sa skladá z počúvania IGMP query otázok z iných smerovačov. Ak je query otázka prijatá s nižšou zdrojovou IP adresou, načúvajúci smerovač zostáva non-query. Ak nie je prijatá žiadna query otázka od iných smerovačov, načúvajúci smerovač sa stáva query. IGMPv2 využíva oproti IGMPv1 dva nové typy správ: [10]

Leave Group Message

Používa sa na zníženie času potrebného pre multicast smerovač na zastavenie prevádzky v prípade, že už nie sú žiadny členovia v skupine. Keď hostiteľ opustí skupinu, pošle Leave group message na 224.0.0.2 (všetky smerovače v skupine). Po obdržaní správy, smerovač pošle sériu group-specific query otázok na hostiteľskú skupinu. Ak žiadny hostiteľ nereaguje na tieto otázky, smerovač rozhodne, že už nie je viac členov v hostiteľskej skupine na danej podsieti a odstráni položku IGMP tabuľky skupinového rozhrania.

Group-Specific Query

Host membership query je posielané na 224.0.0.1 (všetky hostiteľské skupiny), na otázku členstva v skupine hostiteľov v podsieti. IGMPv2 smerovače môžu tiež poslať group-specific query (otázka pre špecifické multicast skupiny odoslaná na skupinovú adresu).

2.3.3 IGMPv3

Je kompatibilná s IGMPv1 aj IGMPv2. Odlišuje sa od nich pridaním zdrojovej filtrácie. To je schopnosť systému vyjadriť svoj záujem o príjem paketov na danú skupinovú adresu len zo špecifických zdrojových adries (režim include) alebo obrátene zo všetkých adries okrem špecifických zdrojových adries (režim exclude). Tieto informácie slúžia smerovačom s podporou pre skupinové smerovanie, aby neposielali pakety zo špecifických zdrojových adries tam, kde nie je záujem o ich prijatie. [3]

Aby bolo plne možné využiť schopnosti IGMPv3, systémové IP služby rozhrania musia podporovať nasledujúcu operáciu:

```
IPMulticastListen(socket, interface, multicast-address,
filter-mode, source-list)
```

Socket je špecifická implementácia parametru používaná k rozlíšeniu medzi rôznymi žiadajúcimi entitami (napr. programy alebo procesy) v systéme. Interface je miestny identifikátor sieťového rozhrania, na ktorom príjem špecifikovanej multicast adresy je povolený alebo zakázaný. Multicast-address je IP multicast adresa alebo skupina, ktorej sa žiadosť týka. Filter-mode definuje, či adresy v source-list sú v režime include alebo exclude. Source-list je neusporiadaný zoznam unicastových adries. [23]

2.3.4 IGMP proxy

Účelom IGMP proxy (zástupca) je umožniť multicast smerovaču, aby sa naučil informácie o členstve v skupine a aby bol schopný prenášať pakety na základe týchto informácií. Je schopný fungovať len v určitých topológiách, ktoré nevyžadujú multicast smerovacie protokoly (DVMRP, PIM-DM a PIM-SM) a majúcich stromovú topológiu, pretože tam nie je žiadna podpora pre funkcie ako spanning tree (rozpätie stromu) na opravu paketových smerovacích slučiek. Proxy obsahuje mnoho explicitne nakonfigurovaných downstream (po prúde) rozhraní a unikátne upstream (proti prúdu) rozhranie. Vykonáva hostovskú stranu IGMP protokolu na jeho upstream rozhraní a stranu smerovača na jeho downstream rozhraniach. IGMP proxy

ponúka mechanizmus pre multicast prenos založený iba na IGMP membership report. Smerovač musí rozhodnúť o odovzdávaní paketov na každom zo svojich rozhraní. Proxy vytvorí presmerovanie položky na základe IGMP membership report a pridá to do multicast prenosovej medzipamäte, aby sa nespravilo rozhodnutie na prenos pre ďalšie multicast pakety s rovnakou kombináciou zdroja a skupiny.[9]

2.3.5 IGMP Snooping

Multicast môže na príslušné porty šíriť len smerovač, pretože sa pozerá do paketov na tretej vrstve. Zariadenia druhej vrstvy (prepínače) pracujú len na úrovni rámcov, preto nemajú prehľad o tom, kto je alebo nie je do danej multicastovej skupiny prihlásený a rozosielajú multicastové rámce na všetky porty. Prepínač, v predvolenom režime, zaplavuje multicastovou prevádzkou všetky porty v broadcastovej doméne. Existujú však mechanizmy, ktoré informujú prepínač o tom, na ktoré porty má multicastové rámce posielať. Jedným z nich je IGMP Snooping. Táto technika skúma obsah IGMP správ. Prepínač, ktorý je toho schopný, teda musí vedieť spracovávať rámce na druhej vrstve, ale musí čiastočne rozumieť aj paketom na tretej vrstve. Ďalej si musí udržiavať vo svojej pamäti tabuľku multicastových MAC adries zo zoznamu portov s účastníkmi prihlásenými do odpovedajúcej multicastovej skupiny. IGMP Snooping prebieha interne na prepínačoch a nie je protokolovou funkciou. Je preto obzlášť vhodný pre multicast aplikácie náročné na šírku pásma. [19]

2.4 Smerovanie v multicaste

Smerovacích protokolov, ktoré umožňujú multicast prenos, je niekoľko. Všetky protokoly využívajú UDP transportný protokol a ich cieľom je nájsť také cesty v sieti, aby multicast prevádzka efektívne dosiahla na každého člena jednotlivých skupín. Skupinové smerovanie sa odohráva prostredníctvom tvorby distribučných stromov (distribution tree). Na rozdiel od bežného smerovania môže mať smerovač viac rozhraní, ktorými posiela datagramy pre určitú skupinu. Distribučný strom má svoj koreň v smerovači a vetvy vedú k členom skupiny. Strom môže byť zdieľaný (shared), kedy všetky zdroje zdieľajú jeden distribučný strom a v ich jadre je stretávací smerovač (rendezvous point). Alebo môže byť strom zdrojový (source), ktorý umožňuje práve jednu cestu od zdroja ku každému cieľu v sieti a každá dvojica zdroj-skupina má svoj nezdieľaný strom.

Multicast smerovacie protokoly sa delia na dense (husté), ktoré používajú zdrojový distribučný strom a zaplavujú sieť datagramami pre skupiny, pokiaľ nie je zaplavovanie explicitne odmietnuté (napr. DVMRP alebo PIM-DM), a sparse (riedke),

ktoré sú založené na explicitnom prihlásení do skupiny (napr. PIM-SM). V prvom prípade je nedostatkom neefektívnosť smerovania a nedostatočná rozšíriteľnosť, v druhom prípade zase komplexnosť. [19]

2.4.1 DVMRP

Skupinový smerovací protokol na bázi vektorov vzdialenosti využíva vlastný smerovací mechanizmus založený na algoritme vektorov vzdialenost. Každý smerovač vysiela obdržaný paket určený skupine všetkými cestami okrem cesty späť ku zdroju, čím sa má zaručiť dosiahnutie každej siete, ale niekedy za cenu niekoľkých kópií paketu. Smerovač dostane naspäť informácie z oslovených sietí o prítomnosti alebo neprítomnosti staníc prislúchajúcich konkrétnej skupine. Distribučný strom sa tak vytvára postupne, nie naraz. DVMRP pôsobí značné problémy zbytočným zaťažovaním siete častým záplavovým smerovaním, preto sa v mnohých prípadoch (hlavne cez oblasti siete, ktoré skupinové vysielanie nepodporujú) používa mechanizmus tunelovania. DVMRP je síce stále častejšie nahradzovaný PIM-SM, ale môžeme sa s ním stretnúť v niektorých starších sieťach (napr. s klasickými prístupovými servermi pre vytáčané spojenia). Podrobnejšie je DVMRP popísaný v RFC 1075 [22].

2.4.2 MOSPF

Multicast OSPF protokol predstavuje rozšírenie protokolu OSPF pre podporu smerovania skupinového vysielania (RFC 1585 [17]). Smerovač posiela LSA o členstve v skupine tak, aby mali všetky smerovače rovnakú znalosť členov skupiny pre danú reláciu skupinového vysielania. V paketoch o stave sa objavuje aj informácia o skupinách aktívnych v jednotlivých sieťových segmentoch. MOSPF si pre každú dvojicu zdrojovej siete a skupiny buduje distribučný strom s koreňom u zdroja. Je to jediný protokol založený na strome najkratších ciest: strom je založený na najnižšej metrike (cost) a buduje sa naraz, nie postupne.

Protokol zaručuje posielanie datgramov len v prípade skutočnej potreby (demand -driven), na rozdiel od princípu protokolu DVMRP (data-driven), preto je zvlášť vhodný pre situácie s relatívne malým počtom aktivných staníc generujúcich datagramy na skupinovú adresu. Nevýhodou je vysoká záťaž smerovača: každý smerovač musí udržovať informácie o všetkých existujúcich skupinách v oblasti a synchronizovať ich, aby všetci mali rovnakú databázu, a prepočítavať strom najkratších ciest pomocou zložitého Djikstrovho algoritmu pri každej zmene členstva. [23]

2.4.3 PIM-DM

Skupinové vysielanie nezávislé na protokole, tzv. hustý režim je smerovací protokol na základe zdroja. Je vhodný v situácii silnej skupinovej prevádzky v sieti s malým počtom zdrojových staníc a značným počtom cieľových staníc v skupinách (aspoň jeden príjemca na segmente pre každú aktívnu skupinu). PIM-DM sa rovnako využíva pri konštantnej skupinovej prevádzke a pri fyzickej blízkosti zdrojov a cieľov skupinového vysielania. Pracuje podobne ako DVMRP, zaplavuje všetky podsiete datagramami určenými skupine (predpokladá rýchle siete s dostatočnou šírkou pásma), pokiaľ nedostane negatívnu odpoveď od smerovača na cieľovej podsieti o neprítomnosti žiadneho člena danej skupiny. PIM-DM potrebuje tradičné smerovacie informácie, musí poznať najkratšie cesty do každého cieľa. Na rozdiel od DVMRP nemá možnosť inzerovať konvenčné cesty. Predpokladá teda, že smerovač sa postará o kvalitnú znalosť topológie siete a výber optimálnych ciest v sieti. [19]

2.4.4 PIM-SM

Skupinové vysielanie nezávislé na protokole, tzv. riedky režim je popísaný v RFC 4601 [8]. V dnešnej dobe je najbežnejšie používaný multicast smerovací protokol. Je vhodný v situácii, keď sa jedná o veľký počet skupín, ale malý počet príjemcov v rámci skupiny, pri rôznorodosti prevádzky a prítomnosti diaľkových spojov. Pracuje v rámci domény, kde doména je skupina smerovačov s podporou pre PIM-SM prepojených fyzickými spojmi alebo tunelmi, ktoré sa dohodnú na rovnakej matici mapovania RP (Rendezvous point). Je založený na požiadavke: na rozdiel od ostatných protokolov predpokladá, že žiadna stanica neočakáva skupinovú komunikáciu, pokiaľ o to sama nepožiada. Akonáhle smerovač obdrží správu IGMP Membership Report od stanice na priamo pripojenej sieti, je zodpovedný za budovanie vetvy stromu pre túto skupinu. Tento posledný smerovač na ceste k cieľu sa označuje ako poverený smerovač (DR, Designated Router) pre príjemcov. DR pošle (*,G) PIM Join správu svojmu susedovi podľa smerovacej tabuľky pre multicast smerovacie protokoly (môže byť zhodná s klasickou smerovacou tabuľkou), aby zistil adresu RP. Správa Join sa posiela na multicast adresu všetkých smerovačov s PIM (224.0.0.13) s TTL=1. Ale pretože správa musí dojsť až k RP, každý smerovač na ceste, ktorý nie je RP, tak ju generujú a posielajú opäť.

Akonáhle sa vybuduje strom RPT (Rendezvous Point Tree), zostáva v platnosti, aj keď sa žiadna prevádzka v skupine negeneruje. Pokiaľ zdroj začne vysielať do skupiny, jeho DR zapuzdruje dáta do datagramu s PIM Register a pošle ho na RP. Ten môže doručiť datagram na skupinovú adresu prostredníctvom RPT všetkým príjemcom, alebo pošle správu (S,G) PIM Join smerom ku zdroju, aby si vybudoval strom najkratších ciest. Hneď po zahájení komunikácie cez miesto stretnutia od zdroja

k príjemcovi, smerovače na ceste dĺžku cesty optimalizujú, pretože RPT samozrejme nemusí predstavovať optimálnu cestu od zdroja ku každému príjemcovi. Po vytvorení stromu najkratších ciest, DR dostáva dve kópie každého datagramu do skupiny: cez RPT a cez strom najkratších ciest. Aby sa tomu zamedzilo a umožnilo optimálne smerovanie, pošle RP správu PIM Prune (prerezanie). Tým informuje RP, že už nemusí posielať datagramy prostredníctvom RPT pre danú dvojicu zdroj-skupina.[19]

3 SLUŽBY ŠÍRENÉ MULTICASTOM

Multicast je technológia, ktorá nám umožnuje doručovať IP pakety od jedného odosielateľa mnohým, avšak vždy jasne vyčleneným príjemcom, preto je jeho využitie hlavne pri videokonferencii, internetovej televízii alebo rozhlase. Významné využitie multicastu je pri distribúcii informácií mnohým, potenciálne neznámym príjemcom naraz (napr. smerovacie a iné protokoly). Ďalšie možné využitie je pri online hrách, prenose objemných dát na pozadí alebo pri službe video on demand. Väčšina týchto služieb by sa nezaobišla bez použitia tohto protokolu:

RTP

Definuje a štandardizuje formát paketov pre prenos aplikácií prenášajúcich dáta v reálnom čase, ako je audio alebo video cez multicast alebo unicast sieťové služby. RTP je akousi nadstavbou nad UDP. Nezaručuje doručenie dát ani správne poradie jednotlivých paketov, ale definuje ich poradové čísla, podľa ktorých môžu multimediálne aplikácie rozpoznať chýbajúce pakety. Bol navrhnutý ako pre prenosy typu multicast, tak pre prenosy typu unicast. Multimediálne streaming (prúdiace) aplikácie v reálnom čase vyžadujú včasnú dodávku informácií a môžu tolerovať nejakú stratu paketov.

Transport dát je doplnený kontrolným protokolom (RTCP), ktorý umožňuje sledovať poskytovanie údajov na veľké multicast siete a zabezpečuje minimálnu kontrolu a identifikačné funkcie. RTP a RTCP sú navrhnuté tak, aby boli nezávislé od základných transportných a sieťových vrstiev. Protokol podporuje použitie dvoch typov vysielačov: translátorov a mixérov. Viac o RTP je možné nájsť v [18].

3.1 Videokonferencie

V poslednom desaťročí sa vďaka obrovskému rozmachu internetu dostali do popredia záujmu pri komunikácii. Podľa typu spojenia sa delia do troch skupín :

- **Konferencia ad-hoc** je základným a najjednoduchším typom konferencie. Začína sa spojením bod-bod, neskôr môže prejsť vo viacbodovú konferenciu.
- **Konferencia bez rezervácie** je alternatívou k plánovaným konferenciám. Vytvára sa vtedy, keď je potrebné rýchlo zostaviť sedenie bez špecifikácie počtu pripojených účastníkov a dobe trvania konferencie.
- **Plánované konferencie** umožňujú špecifikovať zdroje, ktoré budú potrebné pre plánovanú konferenciu. V čase zahájenia konferencie účastník vytočí prístupové číslo pre pripojenie do IVR (Interactive Voice Response) alebo priamo do videokonferenčnej miestnosti. Pri použití IVR je prístup do konferenčnej

miestnosti zaistený pomocou identifikačného čísla. V iných prípadoch môžu byť klientské terminály pozvané do konferencie. K ochrane proti nepovolaným osobám slúži PIN (Personal Identification Number). [4]

Typické centralizované videokonferencie obsahujú vo svojom jadre jednotku, ktorá umožňuje prijímať a preposielať všetky multimediálne toky od účastníkov videokonferencií. Pre transport sa používa nespoľahlivý UDP protokol. U videokonferencie je nízka tolerancia k strate paketov a jitter (vyžaduje sa menší ako 400 milisekúnd). U niektorých kodekových technológií, sú audio (zvuk) a video dáta prenášané v samostatných paketoch. V tomto prípade má audio tok prednosť pred video tokom. Vzhľadom k tomu, oneskorenie by malo byť v prípade audio menšie ako 150 milisekúnd a v prípade videa menšie ako 250 milisekúnd. V iných kodekových technológiách sú audio a video prenášané v rovnakom pakete. Tu sa vyžaduje oneskorenie menšie ako 150 milisekúnd. Pre videokonferencie je určený štandard H.323, ktorý popisuje infraštruktúru audio-vizuálnych služieb v paketovo orientovaných sieťach, ktoré nemôžu zaistiť garantovanú kvalitu služieb. [11]

3.2 IPTV

Je definovaná ako bezpečné a spoľahlivé doručovanie predplatiteľom video zábavy a súvisiacich služieb. Tieto služby môžu napríklad zahŕňať Live TV, video na vyžiadanie (VoD) a interaktívne TV (iTV). IPTV ponúka významné výhody, vrátane schopnosti integrovať televíziu s ďalšími IP-založenými službami ako vysokorýchlostný prístup k internetu a VoIP (Voice over IP). Umožňuje tiež poskytovanie podstatne väčšieho obsahu a funkčnosti. V IPTV jeden program predstavuje práve jednu multicast skupinu, ku ktorej sa môžu potenciálni príjemcovia prihlásiť.

IPTV je citlivá na stratu paketov a oneskorenie ak vysielanie dát je nespoľahlivé. Má prísne požiadavky minimálnej rýchlosti s cieľom uľahčiť správny počet rámcov za sekundu. To znamená, že obmedzená rýchlosť pripojenia a dostupná šírka pásma pre veľké zákaznícke základne môže znížiť kvalitu dodávaných služieb. [2]

3.3 Video on Demand

Služba Video on Demand (video na požiadanie) umožňuje vzdialeným používateľom kedykoľvek prehrať niektoré z veľkých zbierok videa. Typický obsah tvoria filmy alebo filmové nahrávky vybraté z elektronickej videoknižnice. Tieto video súbory sú bežne uložené v sade centrálnych video serverov a distribuované prostredníctvom vysokorýchlostných komunikačných sietí ku geograficky rozptýlených klientov. Základný návrh siete sa skladá z centrálne umiestnenej správy aktív a riadiacich

a kontrolných serverov, ktoré komunikujú so vzdialene umiestnenými Video on Demand diskami cez multicast siete. Po obdržaní žiadosti klienta, server doručí video ku klientovi ako súčasný prúd videa.

Väčšinou je táto služba spoplatnená, preto by mal systém poskytovať účinnú podporu pre ochranu autorských práv pri prenose video prúdov na viac klientov. Služba sa môže používať obmedzený čas. Nezaoberá sa oneskorením pred prehrávaním, ale počas prehrávania. Odpoveď na interaktívne funkcie, ako prehrať a ďalší, by mala byť menšia ako 2-5 sekúnd. Požiadavka na šírku pásma pre backbone (chrbticu) záleží na počte užívateľov, ktorých musí video server podporovať súčasne. Typická šírka pásma v lokálnych sieťach je 1.5 Mb/s. Oneskorenie by nemalo byť menšie ako 150 milisekúnd. [11]

3.4 Internetové rádio

Internetové rádio je systém, pri ktorom je zvuk šírený v digitálnej podobe cez internet. Poskytuje poslucháčom nepretržitý prúd zvuku, ktorý nie je možné pozastaviť alebo opakovane prehrať. Mnoho služieb internetového rádia je spojených so zodpovedajúcou tradičnou (pozemnou) rozhlasovou stanicou, s tým rozdielom, že internetové rádio stanice sú na nich nezávislé. Veľmi výhodným riešením internetového rádia je multicast, kde každý poslucháč upozorní server, že chce počúvať, a server odpovie unikátnym identifikátorom. Služby internetového rádia sú zvyčajne prístupné odkiaľkoľvek na svete. Ponúkajú novinky, šport, diskusie a rôzne žánre hudby, v každom formáte, ktorý je dostupný na tradičných rozhlasových staniciach. [12]

Pre mono-kvalitný MP3 audio prúd je požadovaná šírka pásma 64 kb/s. Pre stereo-kaviltnú MP3 je požadovaná šírka pásma 128 kb/s. Omeškanie (delay) je požadované menšie než 150 ms a jitter by mal byť menší než 100 ms. [11]

3.5 Online hry cez internet

Jednou z možností využitia multicastu je aj hranie online hier. Je to vlastne videohra hraná pomocou osobného počítača alebo hernej konzoly cez internet. Pri online hrách je hojne využívaný multicast. Konkrétne pri veľkom počte hráčov, kde by bolo použitie unicastu nevýhodné, pretože by bolo nutné zasielať pakety zo serveru a na server pomocou unicast. U multimediálnych aplikácií, ako virtuálna realita, by jitter nemal prekročiť 20 - 30 ms. [11]

3.6 Prenos dát na pozadí

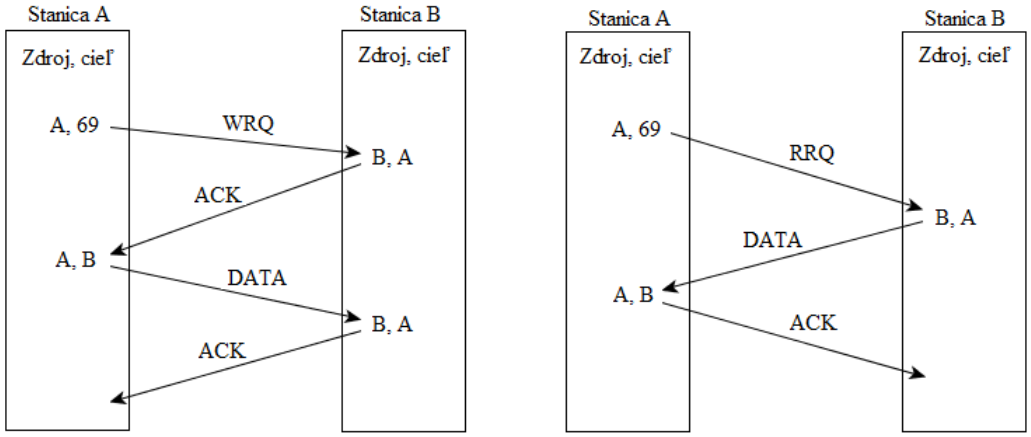
Distribúcia veľkých súborov po sieti z jediného zdroja k veľkému počtu príjemcov nie je efektívna pomocou štandardného klient-server, alebo dokonca peer-to-peer protokolu pre prenos súborov. Preto je prevod hierarchie veľkých súborov na viac miest optimalizovaný z hľadiska využitia šírky pásma a ukladania dát pomocou multicastu. Poskytuje sa mechanizmus pre objednávanie a prenos dát. Systém pre prenos súborov cez multicast sa skladá z dvoch typov entít: odosielateľa a príjemcu. Počas hierarchie prenosu súborov je jediný odosielateľ súborov, ktoré chceme preniesť a mnoho príjemcov, ktorý sa pripoja do rovnakej multicast skupiny.

4 TFTP

TFTP protokol je triviálny sieťový protokol pre prenos súborov. Protokol umožňuje iba čítanie alebo zápis súboru na vzdialenom počítači. Prenos sa uskutočňuje cez bloky pevnej dĺžky, 512 bajtov. Klientská časť protokolu nevyžaduje významné výpočtové zdroje. Server načúva na porte 69. Vzhľadom k tomu TFTP protokol sa často používa pre prenos súborov do LAN smerovačov a prepínačov, a tiež pre načítanie bezdiskových staníc. Tento protokol používa 5 typov paketov:

- požiadavka na čítanie, Read Request (RRQ)
- požiadavka na zápis, Write Request (WRQ)
- dáta, Data (DATA)
- potvrdenie, Acknowledgement (ACK)
- chyba, Error (ERROR)

Zobrazenie vytvorenia spojenia pri požiadavke na zápis a požiadavke na čítanie je na obrázku 4.1.

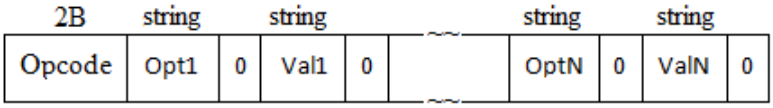


Obr. 4.1: Vytvorenie spojenia pri požiadavku na zápis a na čítanie.

4.1 TFTP pre multicast

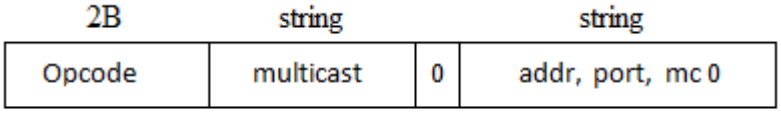
Problematika multicastu v TFTP je zahrnutá v RFC 2090 [7]. V prípade TFTP pre multicast ide o prijímanie toho istého súboru súčasne viacerými klientami. Táto časť zatiaľ nie je súčasťou štandardu, ide o experimentálne rozšírenie protokolu. Popisovaný mechanizmus využíva rozšírenia pôvodnej špecifikácie (TFTP Option Extension), podobne ako napr. dohodnutie dĺžky bloku alebo hodnoty časovača.

Rozšírenia TFTP protokolu umožňujúce dohodnúť pred začatím komunikácie niektoré parametre (napr. dĺžka dátových blokov), sú spätne kompatibilné s pôvodnou špecifikáciou TFTP. Pre potreby dohadovania bol rozšírený formát rámcov RRQ a WRQ. Ak server podporuje dohodnutie parametrov a rospozná niektorý z parametrov uvedený v pakete s požiadavkou (RRQ, WRQ), tak odpovie paketom typu OACK (Options Acknowledgment). Toto je nový typ paketu, ktorý v pôvodnej špecifikácii nebol. Jeho formát je na obrázku 4.2. [13]



Obr. 4.2: TFTP - nový typ paketu.

Pri posielaní žiadosti o čítanie súboru sa pole *Opt* naplní reťazcom multicast, ukončeným nulou. Príslušná položka *Val* je v tomto prípade reťazcom s nulovou dĺžkou. teda nasleduje ďalšia nula. Server odpovedá paketom typu OACK (Opcode = 6), kde v poli *Val* zodpovedajúcom parametru multicast, uvedie trojicu hodnôt addr, port a mc, oddelených čiarkami a ukončených nulou (obr. 4.3).



Obr. 4.3: Paket typu OACK.

addr - multicasová adresa
port - cieľový port multicastových paketov; doporučuje sa použiť registrované číslo 1758 (tftp-mcast)
mc - má hodnotu 0 alebo 1, podľa toho, či tento príjemca bude „Master Client“, teda klient zodpovedný za posielanie potvrdzovacích paketov ACK na server.

4.1.1 Prenos dát

Po prijatí OACK klientom sa pošle serveru paket ACK s číslom bloku 0, čo znamená, že požaduje prvý paket. Inými slovami, ACK môže byť videné ako žiadosť o (n+1)ty blok dát. To umožňuje každému klientovi požadovať ľubovoľný blok v súbore, ktorý mu môže chýbať. Na spravovanie prenosu dát si server udržuje tabuľku klientov, kde „najstarší“ klient je označený ako „Master Client“. Tento „Master Client“ je

zodpovedný za odosielanie ACK na server. Keď master klient ukončí prenos, server odošle ďalšie OACK ďalšiemu najstaršiemu klientovi v poradí, aby začal odosielať ACK. Po obdržaní OACK nový master klient odošle ACK pre blok bezprostredne pred prvým blokom potrebným na dokončenie jeho sťahovania. Počas prenosu môže ktorýkoľvek klient zo zoznamu prijímať pakety požadovaného súboru, ktoré idú cez sieť a potom požadovať všetky chýbajúce bloky, keď sa klient stane master klientom.

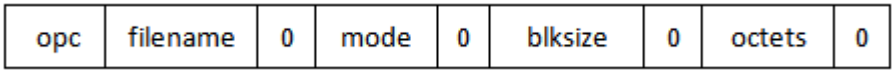
Keď už klient, ktorý potvrdzuje prijaté bloky, ukončí prenos (teda keď už má všetky bloky), tak server pošle paket typu OACK s nastaveným príznakom mc druhému „najstaršiemu“ klientovi. Ten odpovie paketom typu ACK s číslom bloku o jedna menším než číslo bloku, ktorý potrebuje na dokončenie svojho prenosu. Z toho vyplýva, že všetci klienti zbierajú neustále pakety patriace k súboru, ktorý požadovali. Keď sa z nich stanú „Master Client-i“, tak budú požadovať bloky, ktoré sa im zachytiť nepodarilo. Každý klient ukončí prenos potvrdením posledného prijatého paketu. Pakety typu OACK, ktorými server volí nového „Master Client-a“ už môžu mať multicastovú adresu a port nastavené na nulu, pretože ich už klient pozná (z prvého OACK). Ak klient istú dobu neodpovedá, tak server komunikáciu s ním preruší.

Pretože v sieti môže byť viacero serverov, alebo server bude mať obmedzený počet multicastových adries, môže sa stať, že viacero prenosov bude používať tú istú adresu. Preto každý prenos musí mať jedinečné číslo portu, aby sa zaistilo, že každý klient bude prijímať len správne dáta. Zdrojová IP adresa a číslo portu budú identifikovať dátové pakety pre prenos. Preto sú pakety OACK posielané ako unicast, ale musia byť zaslané na ten istý port ako multicastové dáta. [7]

4.2 TFTP Blocksize Option (TFTP možnosť veľkosti bloku)

Základný TFTP protokol pracuje s paketmi veľkosti 512 bajtov dát. Každý paket obsahuje 16-bitový blokový čítač, ktorý začína číslom 1 u prvého bloku. Pokiaľ prenos dát je menší než 65535 blokov (najvyššia hodnota pre 16-bitový čítač), tak je všetko v poriadku. To značí takmer 32 MB.

Pre väčšie súbory je riešením RFC 2348 [14] (TFTP Blocksize Option), ktorý definuje rozšírenie pre väčšie veľkosti bloku. Tento dokument popisuje možnosti TFTP, ktoré umožňujú klientovi a serveru vyjednať použiteľnejšiu veľkosť bloku na sieťovom médiu. TFTP paket so žiadosťou o čítanie alebo zápis je upravený tak, aby obsahoval blocksize option (obr. 4.4), kde sú všetky polia okrem *opc* ukončené nulou.



Obr. 4.4: TFTP paket obsahujúci blocksize option.

Pole *opc* obsahuje buď číslo 1 pre žiadosť na čítanie, alebo 2 pre žiadosť na zápis. Pole *filename* obsahuje názov súboru, ktorý má byť čítaný alebo zapísaný. Pole *mode* obsahuje spôsob prenosu súboru: „netascii“, „octet“ alebo „mail“, bližšie popísané v RFC 1350. V poli *octets* sa nachádza počet oktetov v bloku, špecifikovaných v ASCII (American Standard Code for Information Interchange). Platné hodnoty sú v rozsahu 8 až 65464 oktetov. Blocksize odkazuje na počet dátových oktetov, nezahŕňa 4 oktety TFTP hlavičky.

Ak je server ochotný prijať Blocksize option, odošle OACK (Option Acknowledgment) klientovi. Zadaná hodnota musí byť menšia alebo rovná hodnote špecifikovanej klientom. Klient potom buď použije veľkosť stanovenú v OACK, alebo pošle chybový paket s chybovým kódom 8, aby ukončil prenos. [14]

5 SYSTÉM PRE DISTRIBÚCIU OBSAHU

Pred zahájením distribúcie samotného obsahu som spravil skúšobné meranie vo VirtualBoxe a to pomocou unicastu aj multicastu. Snažil som sa hlavne overiť činnosť RFC 2090, čiže TFTP s podporou multicastu a správanie v prípade zmeny veľkosti bloku (Blocksize option).

5.1 Testovanie vo VirtualBoxe

Meranie prebehlo na mojom vlastnom notebooku pomocou virtualizačného nástroja VirtualBox. V ňom som nainštaloval tri klientské a jeden serverský virtuálny počítač s operačným systémom Debian GNU/Linux. Na testovanie bol použitý súbor *test* s veľkosťou 183 MB. Bolo to z dôvodu, že väčšie súbory by spôsobili príliš veľký počet zachytených paketov vo Wiresharku, ktorý by bol zložitý na spracovanie.

5.1.1 Použité programy

VirtualBox je multiplatformový virtualizačný nástroj distribuovaný ako pre Linux tak pre Windows, ktorý je určený pre podnikanie rovnako ako pre domáce použitie. Je to vysoko výkonný produkt s bohatými funkciami, ktorý je voľne k dispozícii ako Open Source Software (softvér s otvoreným zdrojom). Podporuje veľké množstvo operačných systémov (napr. Windows XP, 7, Linux 2.4, 2.6, Debian, ...). Pre moju prácu som si nainštaloval verziu 4.2.12.

Na všetkých počítačoch je nainštalovaný program *Wireshark*, ktorý je protokolový analyzér a paketový sniffer. Medzi jeho najčastejšie použitie patrí analýza a ladenie problémov v počítačových sieťach, vývoj software, vývoj komunikačných protokolov a štúdium sieťovej komunikácie. Táto aplikácia vie prepnúť sieťovú kartu do promiskuitného režimu a vďaka tomu dokáže zachytávať všetku komunikáciu na pripojenom médiu. Je to multiplatformový software.

Ako TFTP klient bol použitý atftp klient, ktorý nevyžadoval žiadne nastavenie. V prípade TFTP serveru som nainštaloval pokročilý atftpd server, ktorý je založený na špecifikácii RFC 1350, vrátane všetkých rozšírení uvedených v RFC 2347-2349, podporuje tiež multicast. Po nainštalovaní som ho upravil nasledujúcim spôsobom:

```
#mkdir /tftpboot
#chmod 777 /tftpboot
#/etc/init.d/atftpd start
```

Týmto som si vytvoril priečinok `tftpboot`, do ktorého bude možné zapisovať súbory, a z ktorého bude možné sťahovať súbory pomocou TFTP. Do súboru `/etc/inetd.conf` som pridal nastavenie TFTP serveru pomocou tohto riadku:

```
tftp dgram udp4 wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd
--tftpd-timeout 300 --retry-timeout 5 --mcast-port 1758 --mcast-addr
239.2.2.2 --mcast-ttl 10 --maxthread 100 --verbose=5 /tftpboot
```

Nakoniec som zadal príkaz na reštart superserveru inetd:

```
/etc/init.d/inetutils-inetd restart
```

Iperf je bežne používaný sieťový testovací nástroj, ktorý môže vytvoriť TCP a UDP dátové prúdy a merať priepustnosť siete. Je to nástroj pre meranie výkonu siete napísaný v C++. Umožňuje užívateľovi nastaviť rôzne parametre, ktoré môžu byť použité pre testovanie siete. Má funkciu servera aj klienta a môže merať priepustnosť medzi dvoma koncami, a to buď jednosmerne alebo obojsmerne. Je to open source softvér a beží na rôznych platformách vrátane Linux, Unix a Windows.

5.1.2 Testovanie

Ako prvé som testoval unicast prenos. Samotné testovanie prebehlo tak, že prvý klient požiadal server o súbor, a to v termináli pomocou príkazu:

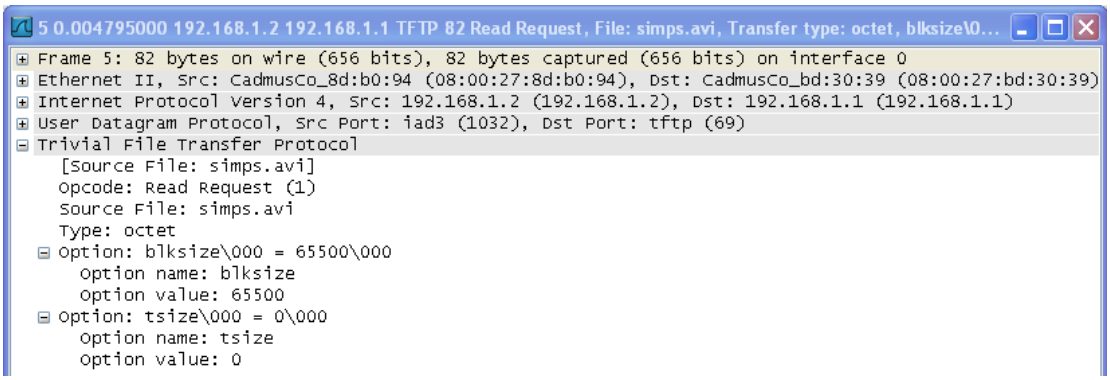
```
atftp -g -r test --blksize 32768 192.168.1.1
```

kde -g v kombinácii s -r je požiadavka na stiahnutie vzdialeného súboru, *test* je požadovaný vzdialený súbor, --blksize je veľkosť bloku nastavená na 32768 oktetov a adresa 192.168.1.1 je adresou TFTP serveru.

Po spustení tohto príkazu klient vyslal správu Read Request (obr. 5.1) smerom na server, ktorou požiadal server o súbor *test*. Server následne odpovedal správou OACK (Option Acknowledgement), v ktorej vyjednal podmienky prenosu. Potom už nasledoval samotný prenos.
Testovanie prebehlo tak, že približne po stiahnutí 25% súboru prvým klientom požiadal druhý klient o ten istý súbor a po 50% tretí. Všetci klienti stiahli celý súbor s rovnakým počtom paketov (5601). Celý prenos všetkých klientov prebehol približne za 80 sekúnd.

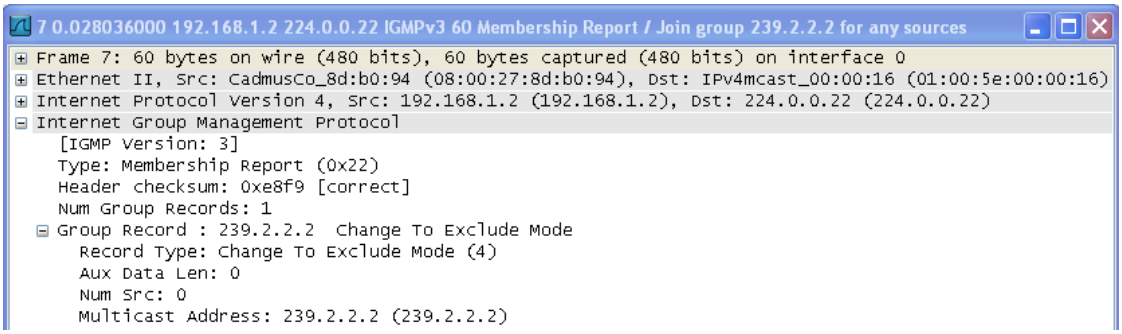
V prípade testovania prenosu pomocou multicastu prvý klient požiadal TFTP server o súbor príkazom:

```
atftp -g -r test --blksize 32768 --multicast 192.168.1.1
```



Obr. 5.1: Správa Read Request od klienta.

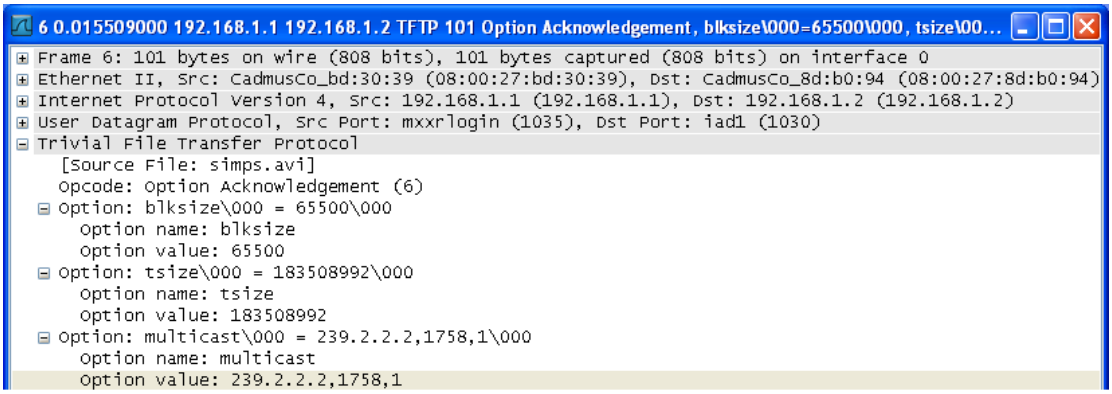
kde takmer všetky voľby sú totožné ako v prípade unicast prenosu. Navyše je parameter --multicast, ktorý znamená požiadavku na multicastový prenos a server je zdroj súborov nastavený na multicastovu adresu 239.2.2.2. Po požiadavke Read Request odpovedal TFTP server správou OACK (obr. 5.3), v ktorej sa oproti unicast prenosu nachádzala možnosť nastavenia multicastu. Server pri možnosti multicast načúval na porte 1758. Po tomto vyjednaní nasledovalo prihlásenie prvého klienta do skupiny pomocou správy Membership report/Join group (obr. 5.2) protokolu IGMPv3. Týmto prihlásením sa prvý klient v poradí stal master klientom. Po úspešnom prihlásení začal prenos samotného súboru zo skupiny, pričom potvrdenia o prijatí paketov boli zasielané na zdroj vysielania a boli vysielané výlučne master klientom.



Obr. 5.2: Správa Membership report/Join group.

Podobne ako pri testovaní unicastu som spustil po stiahnutí 25% súboru sťahovanie druhým klientom a po 50% tretím klientom. Pretože prvý klient bol master klientom, tak ostatní klienti neodosielali ACK správy. Druhý a tretí klient začali sťahovanie paketov v poradí, v ktorom bol aktuálne master klient. Po stiahnutí celého súboru prvým klientom sa novým master klientom stal druhý klient v poradí,

ktorý stiahol a potvrdil chýbajúce pakety. Takto sa to opakovalo, až kým aj posledný klient nestiahol požadovaný súbor. Pre porovnanie, prvý klient potvrdil stiahnutie súboru pomocou 5601 a posledný klient pomocou 1991 TFTP ACK paketov.



Obr. 5.3: Správa OACK (Option Acknowledgement) od serveru.

Veľkú úlohu pri prenose zohrávala aj veľkosť bloku. Predošlý spomínaný prenos prebiehal pri veľkosti bloku 32768 oktetov. V ďalšom testovaní som použil odlišnú veľkosť bloku a testoval som pomocou multicastu. Prvým dvom klientom som nastavil veľkosť bloku 16384 oktetov a druhým dvom som ponechal veľkosť 32768 oktetov. Spustil som súčasný prenos prvého a tretieho klienta, ktorý mali nastavenú odlišnú veľkosť bloku. Po stiahnutí 50% súboru som spustil prenos aj druhých dvoch klientov. V tomto prípade ale prenos prebiehal tak, akoby sa súbor požadoval z odlišnej multicastovej adresy. K tomuto záveru som došiel z toho dôvodu, že v oboch prípadoch sa prvý dvaja klienti stali master klientom, ktorý posielali ACK pakety a zvyšný dvaja čakali, kým prvý klienti stiahnu súbor. Potom sa master klientom stali zvyšný dvaja v poradí.

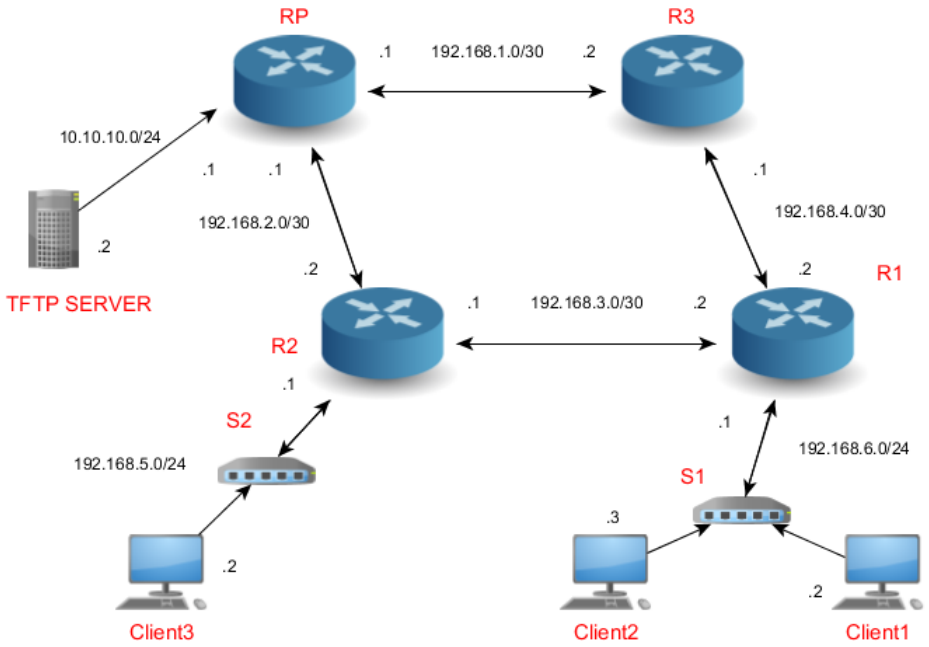
Zistil som, že ak chceme mať v prípade TFTP čo najefektívnejší prenos, tak je dobré mať nastavenú rovnakú veľkosť bloku na všetkých klientoch. V tomto prípade je samozrejme dôležité, aby server podporoval možnosť veľkosti bloku (Blocksize option).

5.2 Systém pre distribúciu

Realizácia samotného systému pre distribúciu obsahu prebehla v laboratóriu použitím smerovačov a prepínačov od firmy MikroTik. Na smerovačoch bežal najnovší RouterOS verzie 5.24, v ktorých bol zahrnutý aj balíček s podporou multicast.

5.2.1 Zapojenie siete

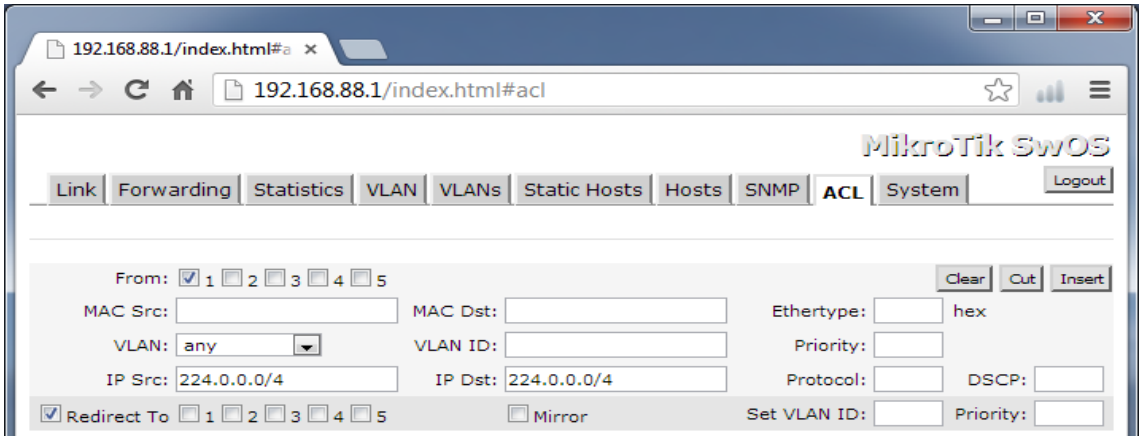
Návrh mojej siete (obr. 5.4) pozostával z dvoch RB750GL a dvoch RB751G smerovačov a dvoch RB250GS prepínačov. K smerovačom R1 a R2 boli pripojení traja klienti, ktorí boli v dvoch podsieťach. K smerovaču RP bol pripojený TFTP server, čiže zdroj vysielania. Už názov napovedá, že smerovač RP bol Rendezvous point.



Obr. 5.4: Schéma zapojenia siete pre distribúciu obsahu.

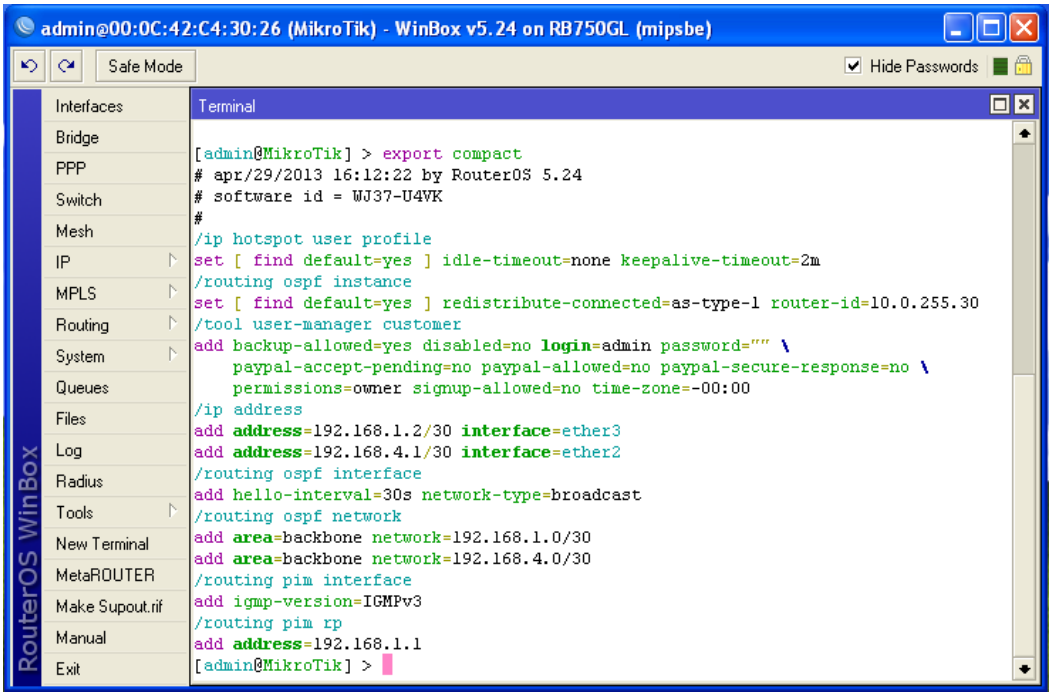
Konfigurácia prepínačov prebehala cez webové užívateľské rozhranie na adrese 192.168.88.1. V tomto rozhraní som z dôvodu, že multicast sa na prepínači správa ako broadcast a Mikrotik prepínače nepodporujú IGMP snooping, nastavil acces list (prístupový zoznam) (obr. 5.5). Je to niečo ako na manuálna konfigurácia IGMP Snoopingu, pretože pomocou tohto nastavenia sa vyfiltruje multicast z portov, kde nechceme zaplavovanie multicast paketmi. V mojom prípade som pomocu položky *Redirect to* zakázal zaplavovanie na všetky porty. Multicast prevádzka bude fungovať len na portoch, kde je to vyžadované. Položka *From* značí rozhranie *ether 1*, ktoré je napojené na smerovač. Položky *IP Src a IP Dst* označujú adresy triedy D, čiže multicast adresy.

Konfigurácia smerovačov prebehla pomocou konzoly Winbox, ktorá sa používa pre prístup k MikroTik konfigurácii a správe smerovača pomocou grafického užívateľského rozhrania (GUI). Príklad skráteného výpisu konfigurácie smerovača R3 je na obr. 5.6. Zvyšné konfigurácie je možné vidieť v prílohe a všetky konfiguračné súbory na priloženom CD. V tejto konfigurácii je vidieť, že ako smerovací protokol som



Obr. 5.5: Príklad acces listu na prepínači S1.

použil OSPF protokol. Na smerovanie multicastu bol použitý PIM protokol s IGMP verziou 3 na všetkých rozhraniach. Ako Rendezvous point je nastavené rozhranie RP smerovača s adresou 192.168.1.1.



Obr. 5.6: Konfigurácia smerovača R3.

5.2.2 Unicast prenos

Ako prvé som realizoval prenos pomocou unicastu. Tento prenos prebehol po zadaní tohto príkazu v termináli každého klienta:

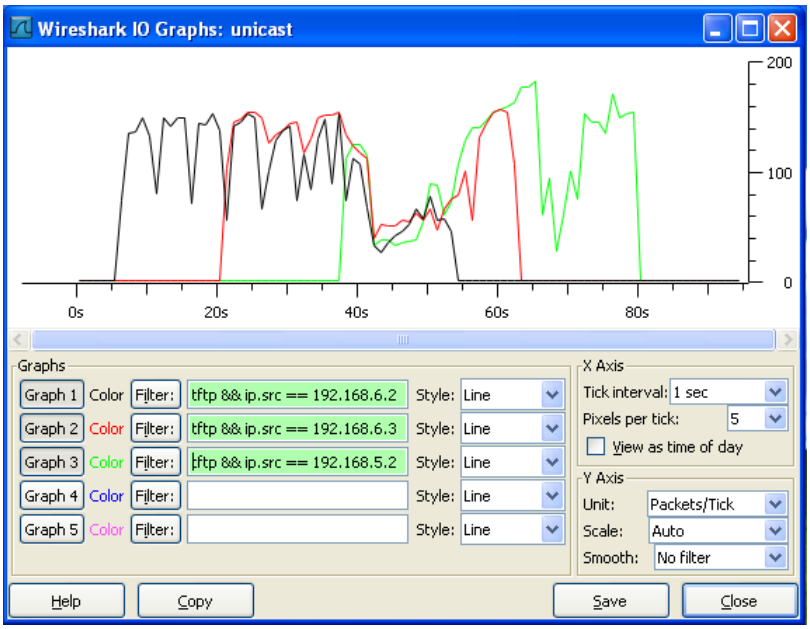
```
atftp -g -r test --blksize 32768 10.10.10.2
```

kde všetky parametre odpovedajú testovaniu vo VirtualBoxe a adresa 10.10.10.2 je adresou TFTP serveru.

Na TFTP serveri som spustil zachytávanie paketov vo Wiresharku. Vo Wiresharku som vyfiltroval a vyobrazil pomocou IO grafu (obr. 5.7) TFTP prevádzku všetkých klientov. Dôležité hodnoty som zadal aj do tab. 5.1. Z grafu je vidieť, že prenos druhého klienta začal približne po 15 sekundách a prenos tretieho klienta po 30 sekundách od začiatku prenosu prvého klienta. Celkový prenos každého klienta prebehol približne za 45 sekúnd.

Tab. 5.1: Unicast prenos

IP adresa	Čas prenosu TFTP	Počet TFTP ACK	TFTP - šírka pásma
192.168.6.2	47 s	5592	0,172 Mbit/s
192.168.6.3	43 s	5545	0,175 Mbit/s
192.168.5.2	44 s	5573	0,168 Mbit/s



Obr. 5.7: Unicast TFTP prevádzka všetkých klientov.

5.2.3 Multicast prenos

Multicast prenos bol podobne relaizovaný pomocou príkazu

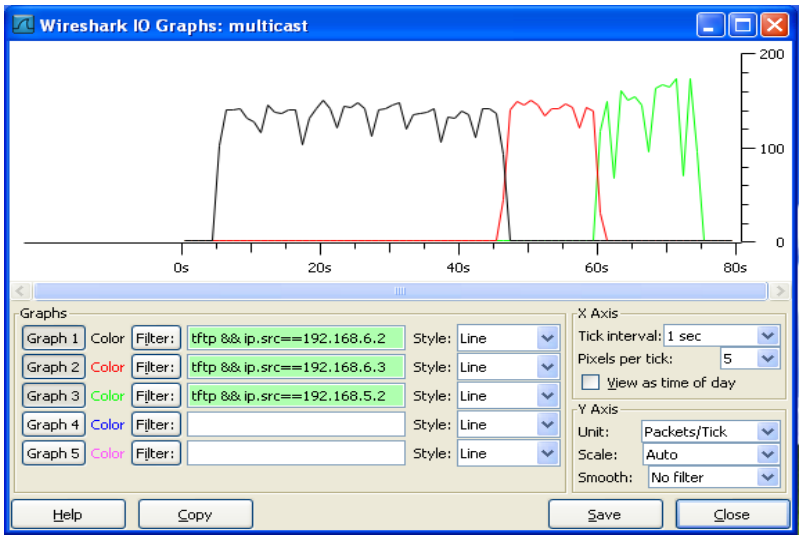
```
atftp -g -r test --blksize 32768 --multicast 10.10.10.2
```

kde všetky parametre sú totožné ako pri testovaní unicastu. Pribudol parameter multicast, ktorý vyjadruje požiadavku na prenos zo serveru pomocou multicastu.

Prenos prebiehal podobne ako u unicastu tak, že prenos druhého klienta začal približne po 15 sekundách a prenos tretieho klienta po 30 sekundách od začiatku prenosu prvého klienta. Opäť som zo serveru pomocou Wiresharku vyfiltroval TFTP prevádzku (obr. 5.8) a dôležité hodnoty zapísal do tab. 5.2. Z grafu je vidieť, že master klientom sa stal prvý klient v poradí. Tento klient odosielal ACK správy na server, pričom prenos ostatných klientov prebiehal súčasne s prvým klientom. Po stiahnutí celého súboru prvým klientom sa stal master klientom druhý klient v poradí. Ten si stiahol len pakety, ktoré mu chýbali. Nakoniec si aj posledný klient v poradí stiahol chýbajúce pakety.

Tab. 5.2: Multicast prenos

IP adresa	Čas prenosu TFTP	Počet TFTP ACK	TFTP - šírka pásma
192.168.6.2	44 s	5562	0,064 Mbit/s
192.168.6.3	15 s	1905	0,022 Mbit/s
192.168.5.2	15 s	2036	0,024 Mbit/s

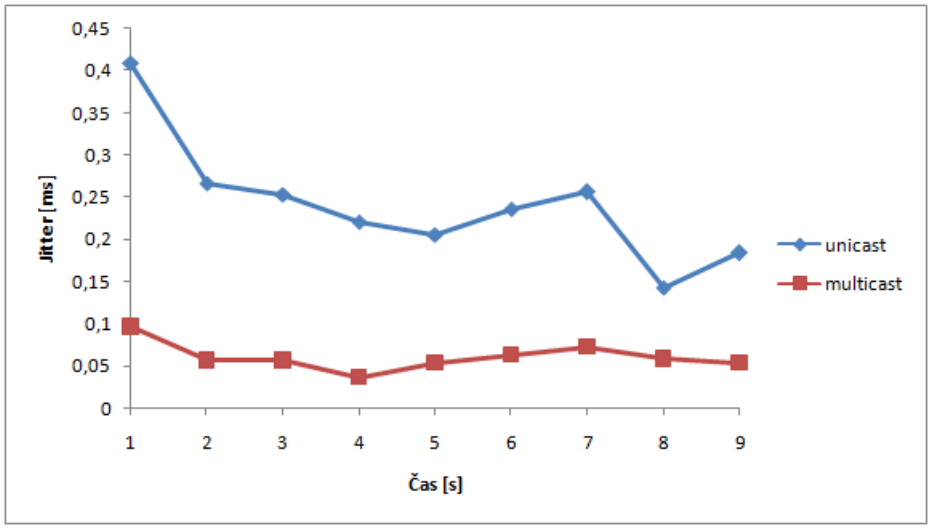


Obr. 5.8: Multicast TFTP prevádzka všetkých klientov.

5.3 Porovnanie unicastu a multicastu

Z môjho merania je vidieť, že už pri relatívne malom súbore (183 MB) sa prejavuje výhoda použitia multicastu oproti unicastu. Značný rozdiel bol vo využitej šírke pásma, kde pre unicast prenos predstavovala celková využitá šírka pásma približne 34,7 Mbit/s a pre multicast prenos 31,3 Mbit/s. V tomto prípade najväšie zlepšenie nastalo v prípade TFTP paketov, kde pre unicast predstavovalo hodnotu 0,391 MBit/s a pre multicast hodnotu 0,061 Mbit/s. Značný rozdiel je vidieť aj z tabuliek 5.1 a 5.2, kde v prípade unicastu boli jednotlivé hodnoty približne rovnaké a v prípade multicastu boli rozdielne a o dosť menšie. V prípade multicastu bola využitá šírka pásma každého klienta oveľa menšia než v prípade unicastu. Tento rozdiel je spôsobený menším počtom potvrdzovacích (ACK) TFTP paketov v prípade multicastu.

Pre porovnanie oboch typov komunikácie som použil aj nástroj Iperf. Testovanie prebehlo pri nastavenej šírke pásma 10 Mbit/s po dobu 9 sekúnd. Po zmeraní bol jediný rozdiel oboch typov komunikácie v jitteri (obr. 5.9). Priemerná hodnota jitteru pre unicast predstavovala 0,242 ms a pre multicast 0,061 ms, čo je približne štvornásobný rozdiel.



Obr. 5.9: Graf závislosti jitteru na čase.

5.4 Cron

Na realizáciu systému pre distribúciu obsahu som si vybral softwarového démona cron. Tento démon v linuxe automatizovane spúšťa v určitý čas nejaký príkaz, resp. proces (skript, program a pod.). Jedná sa vlastne o špecializovaný systémový proces, ktorý v linuxe slúži ako plánovač úloh. Pre ukážku je na každom klientovi nainštalovaný software Adobe Reader vo verzii 9.5.1. Pomocou môjho systému sa automaticky zaktualizuje na verziu 9.5.4.

Architektúra môjho systému spočívala v tom, že na strane klienta sa spustí v určitý čas skript `sync.sh` (musí mať nastavené práva spustiteľnosti (`chmod +x`)):

```
#!/bin/sh
atftp -g -r config.sh --blksize 32768 --multicast 10.10.10.2
chmod +x config.sh
mv config.sh /etc/init.d
/etc/init.d/config.sh start
```

kde `#!/bin/sh` hovorí rodičovskému shellu, ktorý interpret bude použitý na spustenie skriptu. Klient stiahne zo serveru skript `config.sh`. Príkazom `chmod +x` sa pridajú súboru práva na spustenie. Príkazom `mv` sa skript premiestni do súboru `/etc/init.d` a spustí sa pomocou príkazu `start`. Skript `config.sh` obsahuje:

```
#!/bin/sh
ip=‘ifconfig eth0 | grep "inet addr" | grep -o "\([0-9]\{1,3}
\.\?\)\{4\}" | head -n 1‘
export IFS="."
for num in $ip; do
    continue
done
nume=$num

if [ $nume -le 10 ]; then

 if [ -f /home/server/priecinok/AdbeRdr9.5.4-1_i386linux_enu.deb ]
 then
    rm /etc/init.d/config.sh
    exit 0
 else
    atftp -g -r AdbeRdr9.5.4-1_i386linux_enu.deb --blksize 32768
    --multicast 10.10.10.2
    mv AdbeRdr9.5.4-1_i386linux_enu.deb /home/server/priecinok
```

```
 sudo dpkg -i /home/server/priecinok/AdbeRdr9.5.4-1_i386linux_enu.deb
    echo "Inštalácia súboru 2 ukončená." | mail -s
    "Správa od klienta" server@server.workgroup
 fi
else
 exit 0
fi
rm /etc/init.d/config.sh
exit 0
```

Kompletný skript spolu s popisom jednotlivých príkazov sa nachádza na priloženom CD. Pomocou tohto skriptu sa otestuje, či klient patrí do rozsahu IP adries, na ktoré chceme stiahnuť súbor. Toto sa dá využiť pri tom, ak chceme nainštalovať len určité súbory na vybraného klienta. Ďalej sa otestuje, či sa daný súbor už nachádza v počítači. Ak áno, nič sa nestiahne a skript sa ukončí. Inak sa zo serveru stiahne balíček zo softwarom. Príkazmi `sudo dpkg -i` sa s právami superužívateľa rozbalí a nainštaluje nová verzia Adobe Readeru. Po nainštalovaní sa z klienta odošle mail na server, ktorý oznámi serveru, že súbor bol stiahnutý a nainštalovaný. Nakoniec sa príkazom `rm` vymaže stiahnutý skript. Tento skript sa dá ďalej rozšíriť pre inštaláciu viacerých súborov a na viacerých rozdielnych rozsahov klientov.

Všetko sa to riadi pomocu crontab-u. Príkazom `crontab -e` sa upraví jeho nastavenie. V ňom som zapísal:

```
00 12 * * * /etc/init.d/sync.sh
```

Základný formát crontabu je: <minúta> <hodina> <deň v mesiaci> <mesiac> <deň v týždni> <príkaz>. To znamená, že dané skripty budú spustené každý deň o 12:00. Pri opätovnej potrebe urobiť zmenu v systéme jednoducho pozmeníme na serveri v adresári `/tftpboot` skript `config.sh`, kde zadáme žiadosť na stiahnutie potrebného súboru spolu s ďalšími príkazmi pre spustenie alebo nainštalovanie tohto súboru.

5.5 Štart skript

Ďalšou možnosťou systému pre distribúciu je spustenie skriptu počas štartu systému. V tomto prípade je potrebné obsah skriptu `sync.sh` umiestniť do skriptu `/etc/rc.local`. Tento skript je vykonaný na konci každého multi-užívateľského runlevelu (Linux runlevel kontroluje aké procesy/služby sú spustené automaticky systémom). Skript `rc.local` je oproti použitiu `sync.sh` v crone pozmenený:

```
#! /bin/sh
case "$1" in
  start|restart|force-reload)
  atftp -g -r config.sh --blksize 32768 --multicast 10.10.10.2
  chmod +x config.sh
  mv config.sh /etc/init.d
  /etc/init.d/config.sh start
  ;;
  stop)
  ;;
 esac
exit 0
```

Ide o programovú štruktúru, kde sa vykonajú dané funkcie, ak sú vyžadované systémom. Skript `config.sh` je v porovnaní s cronom ten istý. Príkazy bolo potrebné uložiť za časťou skriptu, kde je štart. Je to z dôvodu, aby skript bol spustený na začiatku pri spustení systému a nie pri jeho ukončení.

6 ZÁVEREČNÁ DISKUSIA

Pri testovaní unicast prenosu som zistil, že došlo k menším strátam potvrdzovacích ACK paketov aj po niekoľkých meraniach. Je tu totiž predpoklad, že klienti odošlú rovnaký počet ACK paketov na server, ako je vidieť v tab. 5.1, tak sa tak nestalo.

Pri zapojovaní mojej topológie siete bolo nutné nastaviť manuálny IGMP snooping z dôvodu nefunkčnosti na Mikrotik prepínačoch. Táto možnosť totiž nie je od výrobcu poskytovaná. Najväčším problémom bol dosiaľ navysvetlený výpadok Mikrotik smerovačov. Nefungoval z ničoho nič multicast, preto bola potrebná viacnásobná konfigurácia smerovačov. Odporúčam konfigurovať Mikrotik smerovače jeden po druhom a stále testovať, či multicast funguje. Potom sa dá dopracovať k úspešnej funkčnosti zapojenia.

Testovaním vo VirtualBoxe som zistil, že ak chceme mať v prípade TFTP čo najefektívnejší a najrýchlejší prenos, tak je dobré mať nastavenú rovnakú veľkosť bloku na všetkých klientoch. Odporúčam aj čo najväčšiu veľkosť bloku, a to najlepšie maximálnu veľkosť 65464 oktetov. V tomto prípade je samozrejme dôležité, aby server podporoval možnosť veľkosti bloku (Blocksize option).

Systém pre distribúciu obsahu som realizoval pomocou dvoch spôsobov. A to cronom a pomocou štart skriptu. Hlavný rozdiel medzi nimi bol, že štart skript sa spúšťal pri spustení systému a cron v určitý, mnou vybraný čas. V prípade štart skriptu vidím menší nedostatok v čase spustenia systému, ktorý sa predĺži o čas sťahovania súboru z TFTP serveru. Čiže čím väčší súbor, tým dlhšie spustenie systému. Preto odporúčam skôr cron.

7 ZÁVER

Moja práca by sa dala rozdeliť do dvoch častí. V prvej časti popisujem teoreticky multicast, jeho využitie v paketovo komutovaných sieťach a spôsob adresovania. Ďalej popisujem IGMP protokol, ktorý slúži na prihlasovanie do skupín, kde som popísal aj správanie sa protokolu na prepínači. V práci sa zaoberám aj využitím multicastu a požiadavkami kladenými na sieť pri ich prevádzkovaní. Zistil som, že najväčšie využitie multicastu je pri videokonferenciách a IPTV. Väčšina týchto technológií využíva pri prenose RTP protokol, ktorý slúži na prenos audio a video súborov.

V druhej časti práce som si vybral na prenos dátového obsahu pomocou multicast protokol TFTP. Je to jednoduchý sieťový protokol pre prenos súborov. Tento protokol som využil pri návrhu systému pre distribúciu digitálneho obsahu. Ďalej som spravil testovanie unicastu a multicastu pomocou VirtualBoxu. Potom som realizoval systém pre distribúciu obsahu na vlastnej navrhnutej topológii siete. Vykonal som všetky potrebné merania a pomocou nameraných hodnôt som porovnal obidva prenosy. Zistil som, že multicast prenos využíva oproti unicast prenosu menšiu šírku pásma a taktiež oneskorenie (jitter) vykazuje nižšie hodnoty. Na distribúciu samotného obsahu som využil linuxového démona cron a ako ďalšiu možnosť využitie start skriptov počas štartu systému. Pomocou nich som nastavil automatický prenos a následnu inštaláciu softwaru.

LITERATÚRA

[1] ALBANNA, Z., ALMEROTH, K., MEYER, D., SCHIPPER, M. *RFC 3171 - IANA Guidelines for IPv4 Multicast Address Assignments*. Technická správa, Internet Engineering Task Force, 2001, [cit. 30. 10. 2012]. Dostupné z URL: <http://tools.ietf.org/html/rfc3171>.

[2] ANDERSON, Nate. *An introduction to IPTV*. 13. 3. 2006, [cit. 11. 11. 2012]. Dostupné z URL: <http://arstechnica.com/business/2006/03/iptv/>.

[3] CAIN, B., DEERING, S., KOUVELAS, I., FENNER, B., THYAGARAJAN, A. *RFC 3376 - Internet Group Management Protocol, Version 3*. Technická správa, Internet Engineering Task Force, 2002, [cit. 20. 11. 2012]. Dostupné z URL: <http://tools.ietf.org/html/rfc3376>.

[4] ČÍKA, Petr. skripta: *Multimediální služby*. Brno, 2012, 129 s. ISBN 978-80-214-4443-0.

[5] DAN, Komosný. *Hierarchický Přenos Signalizace pro Multicast v IP Sítích*. Brno: Vutium, 2009, 26 s. ISBN 978-80-214-3833-0.

[6] DEERING, S. *RFC 1112 - Host Extensions for IP Multicasting*. Technická správa, Internet Engineering Task Force, 1989, [cit. 24. 10. 2012]. Dostupné z URL: <http://www.ietf.org/rfc/rfc1112.txt>.

[7] EMBERSON, A. *RFC 2090 - TFTP Multicast Option*. Technická správa, Internet Engineering Task Force, 1997, [cit. 1. 12. 2012]. Dostupné z URL: <http://tools.ietf.org/html/rfc2090>.

[8] FENNER, B., HANDLEY, M., HOLBROOK, H., KOUVELAS, I. *RFC 4601 - Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*. Technická správa, Internet Engineering Task Force, 2006, [cit. 27. 2. 2013]. Dostupné z URL:<https://tools.ietf.org/html/rfc4601>.

[9] FENNER, B., HE, H., HABERMAN, B., SANDICK, H. *RFC 4605 - Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding (ÏGMP/MLD Proxying")*. Technická správa, Internet Engineering Task Force, 2006, [cit. 22. 11. 2012]. Dostupné z URL: <http://www.ietf.org/rfc/rfc4605.txt>.

[10] FENNER, W. *RFC 2236 - Internet Group Management Protocol, Version 2*. Technická správa, Internet Engineering Task Force, 1997, [cit. 20. 11. 2012]. Dostupné z URL: <http://tools.ietf.org/rfc/rfc2236.txt>.

[11] CHEN, Yan, FARLEY, Toni, YE, Nong. *QoS Requirements of Network Applications on the Internet*. 2004, [cit. 10. 11. 2012]. Dostupné z URL:<https://wiki.internet2.edu/confluence/download/attachments/10682402/Ye_48B.pdf>.

[12] KOZAMERNIK, Franc, MULLANE, Michael. *An introduction to Internet Radio*. 26. 10. 2005, [cit. 11. 11. 2012]. Dostupné z URL: <http://www.ebu.ch/fr/technical/trev/trev_304-webcasting.pdf>.

[13] MALKIN, G., HARKIN, A. *RFC 1782 - TFTP Option Extension*. Technická správa, Internet Engineering Task Force, 1995, [cit. 4. 12. 2012]. Dostupné z URL: <http://tools.ietf.org/html/rfc1782>.

[14] MALKIN, G., HARKIN, A. *RFC 2348 - TFTP Blocksize Option*. Technická správa, Internet Engineering Task Force, 1998, [cit. 20. 2. 2013]. Dostupné z URL: <http://tools.ietf.org/html/rfc2348>.

[15] MEYER, D., LOTHBERG, P. *RFC 2770 - GLOP Addressing in 233/8*. Technická správa, Internet Engineering Task Force, 2000, [cit. 15. 11. 2012]. Dostupné z URL: <http://tools.ietf.org/html/rfc2770>.

[16] MEYER, D. *RFC 2365 - Administratively Scoped IP Multicast*. Technická správa, Internet Engineering Task Force, 1998, [cit. 17. 11. 2012]. Dostupné z URL: <http://www.ietf.org/rfc/rfc2365.txt>.

[17] MOY, J. *RFC 1585 - MOSPF: Analysis and Experience*. Technická správa, Internet Engineering Task Force, 1994, [cit. 27. 2. 2013]. Dostupné z URL: <http://tools.ietf.org/html/rfc1585>.

[18] PERKINS, Colin. *RTP: Audio and Video for the Internet*. Boston: Addison-Wesley, 2003, 414 s. ISBN 06-723-2249-8.

[19] PUŽMANOVÁ, Rita. *TCP-IP v kostce*. České Budějovice: Kopp nakladatelství, 2009, 619 s. ISBN 978-80-7232-388-3.

[20] PUŽMANOVÁ, Rita. *Věčné téma: přepojovaní okruhů či paketů? (1)*. 2006, [cit. 18. 10. 2012]. Dostupné z URL: <http://www.svetsiti.cz/clanek.asp?cid=Vecne-tema-prepojovani-okruhu-ci-paketu-1-1842006>.

[21] PUŽMANOVÁ, Rita. *Věčné téma: přepojovaní okruhů či paketů? (2)*. 2006, [cit. 18. 10. 2012]. Dostupné z URL: <http://www.svetsiti.cz/clanek.asp?cid=Vecne-tema-prepojovani-okruhu-ci-paketu-2-1942006>.

[22] WAITZMAN, D., PARTRIDGE, C., DEERING, S. *RFC 1075 - Distnace Vector Multicast Routing Protocol*. Technická správa, Internet Engineering Task Force, 1988, [cit. 27. 2. 2013]. Dostupné z URL: <`http://www.ietf.org/rfc/rfc1075.txt`>.

[23] WITTMANN, Ralph and Martina ZITTERBART. *Multicast Communication: Protocols and Applications*. San Francisco: Morgan Kauffman Publishers, 2001, 349 s. ISBN 15-586-0645-9.

ZOZNAM SKRATIEK

BGP (Border Gateway Protocol)

DNS (Domain Name System)

DVMPR (Distance Vector Mulicast Routing Protocol)

GDA (Group Destination Address)

GUI (Graphical User Interface)

IGMP (Internet Group Management Protocol)

IP (Internet Protocol)

IPTV (Internet Protocol Television)

ISDN (Integrated Service Digital Network)

LSA (Link-State Advertisement)

MAC (Media Access Control)

MOSPF (Multicast Open Shortest Path First)

MPLS (Multi-protocol Label Switching)

OSPF (Open Shortest Path First)

PIM-DM (Protocol Independent Multicast - Dense Mode)

PIM-SM (Protocol Independent Multicast - Sparse Mode)

RTP (Real-time Transport Protocol)

TCP (Transmission Control Protocol)

TTL (Time To Live)

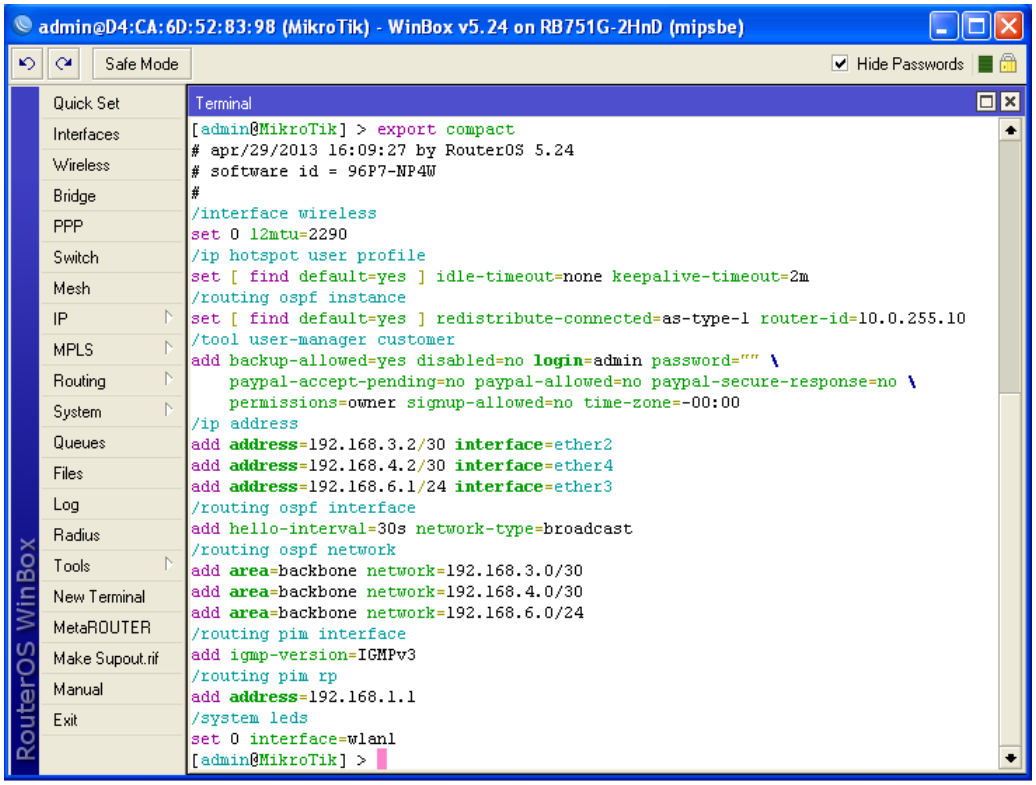
UDP (User Datagram Protocol)

ZOZNAM PRÍLOH

A KONFIGURÁCIE SMEROVAČOV

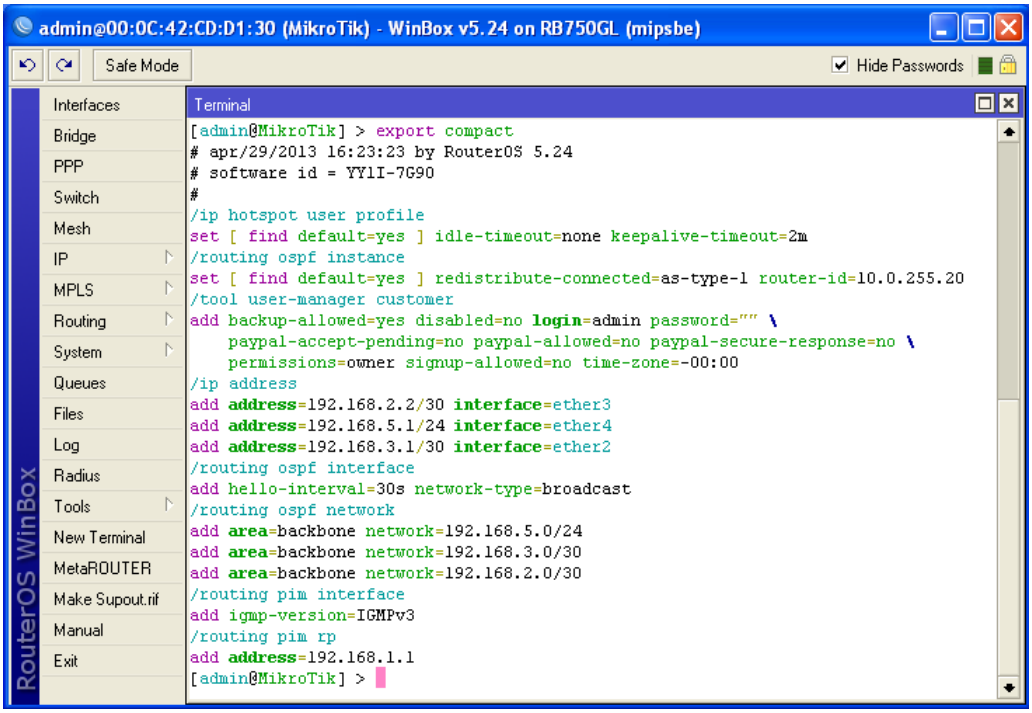
Dané konfigurácie sú výpisom z MikroTik smerovačov pomocou príkazu `export compact`, kde sa zobrazuje len vlastná konfigurácia bez predvolenej konfigurácie. Kompletné konfiguračné súbory sa nachádzajú na priloženom CD. Okrem nich sa tam nachádza aj kompletný skript `config.sh`, ktorý je navyše prepísaný aj do textového súboru.

A.1 R1



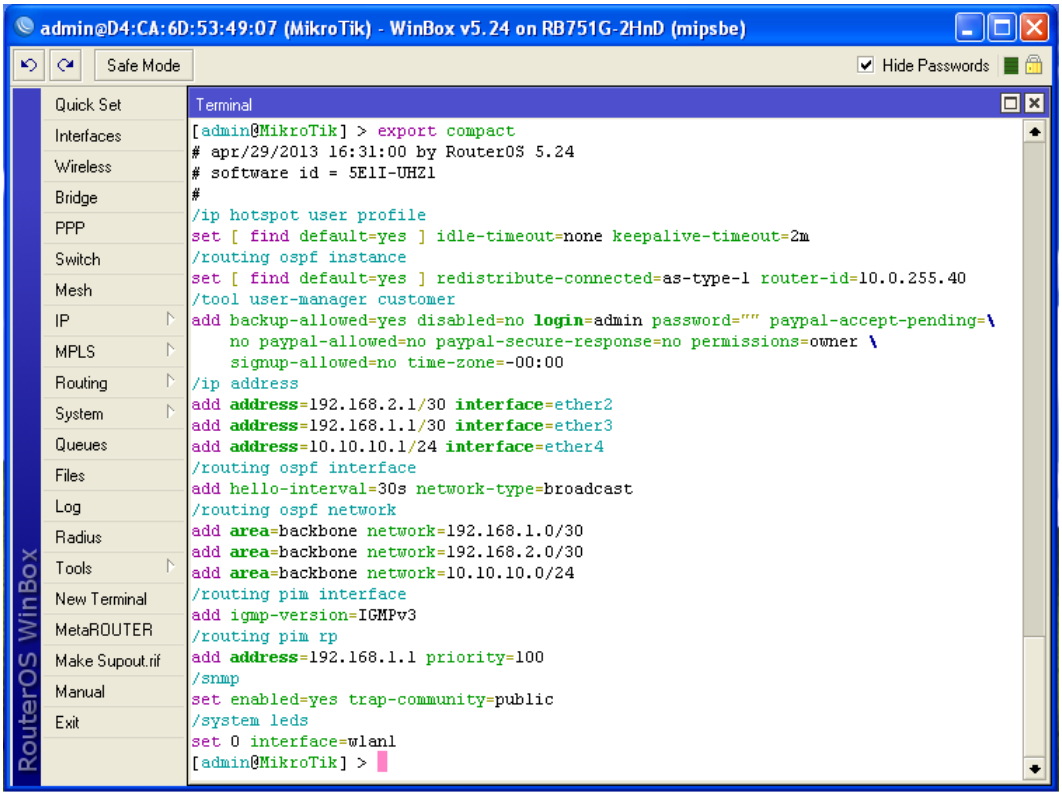
Obr. A.1: Konfigurácia smerovača R1.

A.2 R2



Obr. A.2: Konfigurácia smerovača R2.

A.3 RP



Obr. A.3: Konfigurácia smerovača RP.